UNIVERSIDADE MUNICIPAL DE SÃO CAETANO DO SUL
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE MESTRADO EM ADMINISTRAÇÃO

ABNER DA SILVA NETTO

GESTÃO DA SEGURANÇA DA INFORMAÇÃO:
FATORES QUE INFLUENCIAM SUA ADOÇÃO EM PEQUENAS E MÉDIAS EMPRESAS

São Caetano do Sul
2007

FICHA CATALOGRÁFICA

Silva Netto, Abner da
Gestão da Segurança da Informação: fatores que influenciam sua adoção em pequenas e médias empresas / Abner da Silva Netto. São Caetano do Sul, 2007.

104 f.

Dissertação de mestrado - Universidade Municipal de São Caetano do Sul – IMES. Programa de Mestrado em Administração.
Orientador: Prof. Dr. Marco Antonio Pinheiro da Silveira

1. Informação (Segurança) 2. Empresas (Pequenas e médias)
3. Normas (ISO 17799) I. Título

CDD 005.8

ABNER DA SILVA NETTO

GESTÃO DA SEGURANÇA DA INFORMAÇÃO:
FATORES QUE INFLUENCIAM SUA ADOÇÃO EM PEQUENAS E MÉDIAS EMPRESAS

Dissertação apresentada ao Programa de Mestrado em Administração da Universidade Municipal de São Caetano do Sul como requisito parcial para a obtenção do título de Mestre em Administração.

Área de Concentração: Gestão da Regionalidade e das Organizações.

Orientador: Prof. Dr. Marco Antonio Pinheiro da Silveira

São Caetano do Sul
2007

UNIVERSIDADE MUNICIPAL DE SÃO CAETANO DO SUL
CAMPUS II – Rua Santo Antonio, 50 – Centro – São Caetano do Sul (SP)

Reitor:
Prof. Dr. Laércio Baptista da Silva

Pró-Reitor de Pós-graduação e Pesquisa:
Prof. Dr. René Henrique Licht

Coordenador do Programa de Mestrado em Administração:
Prof. Dr. Eduardo de Camargo Oliva

Dissertação defendida e aprovada em 04/05/2007 pela Banca Examinadora constituída pelos professores:

Prof. Dr. Marco Antonio Pinheiro da Silveira

Prof. Dr. Mauro Neves Garcia

Prof. Dr. César Alexandre de Souza

Aos meus queridos pais, Edite e José, pelo carinho, dedicação, respeito e exemplo de vida. Ao professor e amigo Orlando Dal Degran Jr. pelo incentivo e a oportunidade de lecionar no ensino superior.

AGRADECIMENTOS

Muitas pessoas ajudaram e incentivaram a realização deste trabalho, em especial minha namorada Graziele Meniti por entender meus momentos de ausência nos longos finais de semana longe de sua presença.

Meu orientador e professor Marco Pinheiro pela paciência, por acreditar em meu trabalho, por deixar expor minhas idéias e questioná-las quando necessário. Responsável final pela qualidade deste trabalho.

Ao professor Eduardo Diniz da Fundação Getúlio Vargas, por suas considerações seguras e pertinentes sobre o tema durante a qualificação. Ao professor Antonio Carlos Gil pelas aulas proveitosas e animadas de metodologia científica, por compartilhar comigo um pouco de seu vasto conhecimento e pela grande ajuda no entendimento do meu problema de pesquisa. Aos professores César Alexandre de Souza e Mauro Neves por suas considerações na banca de defesa que ajudaram que esse trabalho tivesse uma maior qualidade nas análises estatísticas. E ao professor Dirceu que muito ajudou na elaboração dos testes estatísticos usando o software SPSS. A todos esses grandes mestres, meu muito obrigado!

A todos meus queridos amigos e colegas de profissão – professores, administradores, técnicos - pela força e incentivo. Especialmente aos grandes amigos Glauber Gonçalves Biazzoto e Fabiano Cutigi Ferrari que estiveram sempre dispostos a ouvir minhas considerações.

Não posso deixar de registrar meus agradecimentos também a toda minha equipe da Enygma Tecnologia: Edmilson, Fernanda, Adonis, Eduardo e Danilo. Especialmente a Fernanda que realizou grande parte das ligações às empresas e ao Adonis pela programação do questionário *web*. Muito obrigado!

LISTA DE GRÁFICOS

Gráfico 1: evolução dos ataques externos reportados no Brasil 20
Gráfico 2: cargo 66
Gráfico 3: departamento 67
Gráfico 4: decisão de compra 67
Gráfico 5: número de empregados 68
Gráfico 6: quantidade de computadores 68
Gráfico 7: responsabilidade da área de TI 69
Gráfico 8: nível de informatização 69
Gráfico 9: camada física 72
Gráfico 10: camada lógica 73
Gráfico 11: camada humana 75
Gráfico 12: grau de importância das ferramentas/técnicas 76
Gráfico 13: avaliação de segurança nas três camadas 78
Gráfico 14: histograma de utilização de ferramentas/ técnicas 79
Gráfico 15: avaliação de segurança nas três camadas por porte de empresa. 80
Gráfico 16: fatores motivadores 84
Gráfico 17: fatores inibidores 85
Gráfico 18: fatores motivadores com a existência da área de TI interna 88
Gráfico 19: fatores inibidores com a existência da área de TI interna 88
Gráfico 20: fatores motivadores de acordo com o tamanho da empresa 90
Gráfico 21: fatores inibidores de acordo com o tamanho da empresa 90
Gráfico 22: fatores motivadores na análise quantidade de computadores 92
Gráfico 23: fatores inibidores na análise quantidade de computadores 92
Gráfico 24: fatores motivadores na análise nível de informatização 94
Gráfico 25: fatores inibidores na análise nível de informatização 94

LISTA DE TABELAS

Tabela 1: distribuição por atividade de pequenas e médias empresas 58
Tabela 2: camada física 70
Tabela 3: camada lógica 72
Tabela 4: camada humana 74
Tabela 5: principais ferramentas ou técnicas que as empresas não possuem implantadas 80
Tabela 6: aderência às seções da norma ISO 17799 81
Tabela 7: fatores motivadores e inibidores 83
Tabela 8: teste *Mann-Whitney* 84
Tabela 9: área de TI interna 87
Tabela 10: teste *Mann-Whitney – Área de TI interna* 87
Tabela 11: tamanho da empresa 89
Tabela 12: teste *Kruskal Wallis – Tamanho da Empresa* 89
Tabela 13: teste *Mann-Whitney – Pequena Empresa* 89
Tabela 14: quantidade de computadores 91
Tabela 15: teste *Kruskal Wallis – Quantidades de Computadores* 91
Tabela 16: teste *Mann-Whitney – Acima de 20 micros* 91
Tabela 17: nível de informatização dos negócios 93

Tabela 18: teste *Kruskal Wallis – Nível de Informatização dos Negócios* 93
Tabela 19: teste *Mann-Whitney – Nível de Informatização Médio* 93

LISTA DE FIGURAS

Figura 1: componentes do risco e medidas de proteção usadas para reduzi-lo. 24
Figura 2: escopo da solução de segurança da informação em camadas..... 33

LISTA DE QUADROS

Quadro 1: normas ISO série 27000..... 46
Quadro 2: comparação entre o modelo de Adachi e Diniz e a norma ISO 17799 47
Quadro 3: comparação entre os domínios de Sêmola e Beal e a norma ISO 17799 47
Quadro 4: seções da norma ISO 17799 por camadas 48
Quadro 5: estágios de crescimento de TI, segundo Nolan..... 55
Quadro 6: principais contribuições das entrevistas 63
Quadro 7: conjunto de variáveis..... 64

SUMÁRIO

1 INTRODUÇÃO 10

2 REFERENCIAL TEÓRICO 14
2.1 Conceito de Segurança da Informação 14
2.1.1 Implementação da Gestão da Segurança da Informação 17
2.1.2 Informações Recentes sobre Segurança da Informação 19
2.2 O Valor das Informações 21
2.3 Gerenciamento do Risco 23
2.3.1 Ameaças 25
2.3.2 Técnicas de Defesa 28
2.4 Camadas de Segurança da Informação 31
2.4.1 Camada Física 33
2.4.2 Camada Lógica 34
2.4.3 Camada Humana 36
2.5 Normas e Padrões de Segurança 37
2.5.1 COBIT 37
2.5.2 ABNT NBR ISO/IEC 17799:2005 37
2.5.2.1 Seções e Controles da Norma 17799:2005 40
2.5.3 ISO/IEC 27001 45
2.6 Domínios da Segurança da Informação 47
2.7 Concepções errôneas acerca da segurança 50
2.8 Tecnologia da Informação em pequenas e médias empresas 51
2.9 Fatores influenciadores para adoção de TI em pequenas e médias empresas 53

3 METODOLOGIA 57
3.1 Tipo de Pesquisa 57
3.2 Amostra e Sujeitos da Pesquisa 57
3.3 Instrumento da Pesquisa 58
3.3.1 Entrevistas para Criação do Questionário 59
3.3.2 Principais Resultados das Entrevistas 60
3.3.3 Questionário 63
3.4 Procedimentos para Coleta de Dados 64
3.5 Procedimentos para Análise dos Resultados 65

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS 66
4.1 Caracterização da Amostra 66
4.2 Ferramentas e Técnicas de Gestão da Segurança da Informação 70
4.2.1 Camada Física 70
4.2.2 Camada Lógica 72
4.2.3 Camada Humana 74
4.3 Gestão da Segurança da Informação nas Três Camadas 78
4.4 Aderência às seções da norma ISO 17799 80
4.5 Fatores motivadores e inibidores 82
4.5.1 Área de TI interna 87

4.5.2 Tamanho da empresa 89
4.5.3 Quantidade de computadores 91
4.5.4 Nível de informatização dos negócios 93

5 CONCLUSÃO 95

6 REFERÊNCIAS 97

RESUMO

Este estudo teve como objetivos: 1. verificar em que medida as pequenas e médias empresas realizam gestão da segurança da informação e 2. identificar fatores que influenciam pequenas e médias empresas a adotarem medidas de gestão da segurança da informação. Foi realizada pesquisa de natureza exploratório-descritiva, e utilizou-se como delineamento o levantamento (*survey*). A amostra consistiu em 43 indústrias do setor de fabricação de produtos de metal situadas na região do grande ABC. Com base na literatura sobre gestão da segurança da informação e na norma brasileira de segurança da informação, foram identificadas as ferramentas ou técnicas de gestão da segurança da informação e classificadas em três camadas: física, lógica e humana. O estudo identificou que a camada humana é a que apresenta a maior carência de cuidados por parte das empresas, seguida pela camada lógica. O antivírus é a ferramenta/técnica mais utilizada pelas empresas pesquisadas para garantir a segurança da informação. A pesquisa relevou que 59% das empresas pesquisadas possuem um nível de segurança satisfatório e que o principal fator motivador para adoção de gestão da segurança da informação é "evitar possíveis perdas financeiras". Todos os fatores inibidores se mostraram importantes para as empresas pesquisadas: falta de conhecimento, valor do investimento, dificuldade em mensurar custo/ benefício, cultura organizacional.

ABSTRACT

The objectives of this study were: 1. verify in what measure the small and medium companies accomplish the management security information and 2. identify which factors influence the small and medium companies to adopt measures of management security information. The source research was exploratory-descriptive and the design was used to the survey. The sample was compound of 43 metal production industries located in ABC region. According to management information security literature and Brazilian norm of information security were identified the tools or techniques of management security information and classified it into three layers: physic, logic and human. The study identified that the human layer is the one that presents the major shortage of cares in the companies followed by the logical one. The companies get used to have the antivirus as the main security tool/technique according to the researched companies to guarantee the safety of information. Besides that, the research showed that 59% of the companies have a safety satisfactory level and the main motivator factor to adopt the management security information is "to avoid possible financial loss". On the other hand, all the inhibitors factors showed important to the researched companies like: lack of knowledge, investments value, organization culture and difficulty to measure cost/benefit.

1 INTRODUÇÃO

Com a utilização dos computadores em diversas organizações, as informações começaram a se concentrar em um único lugar e o grande volume dessas informações passou a ser um problema para a segurança. Os riscos aumentaram com o uso dos microcomputadores, a utilização de redes locais e remotas, a abertura comercial da Internet e a disseminação da informática para diversos setores da sociedade.

> De forma geral, os mesmos riscos presentes em um ambiente de grandes computadores também existem em ambientes de microcomputadores ou redes, porém, devido à arquitetura aberta das plataformas do tipo PC e similares esses equipamentos e seus softwares são essencialmente inseguros. (CARUSO e STEFFEN, 1999).

A expansão da microinformática e seu uso cada vez mais freqüente nos negócios, principalmente por pessoas com pouco ou nenhum conhecimento aprofundado em Tecnologia da Informação (TI), implica riscos crescentes à segurança da informação uma vez que os microcomputadores aumentam a capacidade de processamento, facilidade de uso, armazenamento de dados e compartilhamento de informações, com a conseqüente dependência de muitas organizações em relação aos mesmos.

Embora as organizações tenham-se beneficiado desse avanço e principalmente do uso da Internet, utilizando sua infra-estrutura para economizar custos de comunicação, facilidades na divulgação de produtos, ganho de tempo na maior agilidade das operações com bancos, fornecedores e clientes, a Internet é de uso público o que a torna disponível praticamente a qualquer pessoa, podendo ser utilizada com má intenção. Portanto, a segurança das informações das empresas fica comprometida e fácil de ser explorada, tornando-se assim importante gerenciá-la para uso eficiente dos seus sistemas internos e a garantia da continuidade do negócio.

Origem do Estudo

A gestão da segurança da informação trata-se de um tema importante para as empresas e seus gestores, devido ao fato da informação ser um recurso necessário para o sucesso de praticamente qualquer tipo de negócio atual. Com a maior divulgação de incidentes e fraudes envolvendo informações armazenadas em

recursos de tecnologia, a maior disseminação dos conceitos e ferramentas de segurança da informação e sua utilização cada vez mais freqüente pelas organizações independentemente de seu porte, o tema ganhou relevância empresarial nos últimos anos. Este trabalho busca o aperfeiçoamento de conhecimentos a fim de contribuir com a comunidade acadêmica e empresarial para melhor entendimento do assunto visando descrever os principais motivos que levam as organizações a adotarem controles e medidas para gestão da segurança da informação.

Com o acompanhamento da evolução da informática desde a década de 90, principalmente em pequenas e médias empresas, foi possível acompanhar o processo de informatização de algumas organizações e a evolução das redes computacionais. A abertura comercial da Internet, antes restrita a poucas universidades, tornou o estudo das redes mais relevante porque ampliou seus vários benefícios de comunicações às organizações do mundo todo. Entretanto, logo surgiram problemas de fraudes, roubo e crimes, utilizando-se das facilidades das redes e da Internet o que despertou o interesse para os problemas de segurança da informação, suas técnicas, ferramentas, ameaças e sua correta gestão.

Problematização

O problema de pesquisa tratado neste trabalho é: **Que fatores são capazes de influenciar a adoção da gestão da segurança da informação por pequenas e médias empresas?**

Objetivo

O objetivo geral deste trabalho é identificar os fatores que influenciam pequenas e médias empresas a adotarem medidas de gestão da segurança da informação e avaliar o grau de importância deles.

Outro objetivo é descrever, através dos controles contidos na norma brasileira de segurança da informação ABNT NBR ISO/IEC 17799:2005 (Tecnologia da Informação – Técnicas de Segurança e Código de Práticas para a Gestão da Segurança da Informação), se as empresas pesquisadas possuem requisitos mínimos e satisfatórios de gestão da segurança da informação. Para tanto, os controles descritos na norma foram classificados em três camadas: física, lógica e

humana. A empresa considerada “satisfatória” deve possuir controles efetivos nas três camadas.

Justificativa

Este estudo mostra-se importante porque pouca literatura referente à adoção da gestão da segurança da informação foi encontrada, principalmente em pequenas e médias empresas do Brasil. Assim, o desenvolvimento de pesquisas sobre o tema pode fornecer resultados que ajudem a melhor compreender o valor das informações empresariais, os riscos e as ameaças, o impacto nos negócios e os fatores motivadores ou inibidores relacionados a sua adoção em pequenas e médias empresas.

A gestão da segurança da informação ganha a cada dia maior foco por parte dos gestores e mídias especializadas, com a publicação da norma ABNT NBR ISO/IEC 17799:2005 e da norma ABNT NBR ISO/IEC 27001:2006; uma com o intuito de normalizar e a outra, de certificar um Sistema de Gestão da Segurança da Informação (SGSI) devem ganhar maior adoção por organizações de todos os portes. A gestão da segurança da informação envolve não só recursos tecnológicos, mas também recursos humanos e culturais da organização. Assim sua correta gestão pode ajudar a evitar fraudes financeiras, perda da imagem e confiança por parceiros, fornecedores e clientes.

Delimitação do Estudo

Esse trabalho estudou as pequenas e médias empresas industriais presentes na região do Grande ABC, composta pelas cidades de: Santo André, São Bernardo do Campo, São Caetano do Sul, Diadema, Mauá e Ribeirão Pires.

Várias categorizações existem para definir o porte da empresa. O Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte, instituído pela Lei Complementar nº 123 de 14/12/2006, utiliza o valor do faturamento anual. O Serviço Brasileiro de Apoio à Microempresa (SEBRAE) além de utilizar o faturamento, utiliza-se também do número de pessoas ocupadas. Para este trabalho a categorização usada para pequenas e médias empresas foi o número de empregados, conforme definido pelo Centro de Indústria do Estado de São Paulo (CIESP), sendo:

- pequena empresa - de 10 a 99 empregados;
- média empresa - entre 100 e 499 empregados.

Vinculação à Linha de Pesquisa

Esta pesquisa se vincula à Linha 2 do Programa de Mestrado em Administração da Universidade Municipal de São Caetano do Sul - IMES: Gestão e Inovação Organizacional, pelo fato de tratar assuntos ligados a gestão empresarial e adoção de novas tecnologias.

2 REFERENCIAL TEÓRICO

Para construção do referencial teórico deste trabalho, primeiramente foi pesquisado na literatura da área o conceito de segurança da informação e os dados mais recentes sobre incidentes envolvendo o tema; em seguida procurou-se levantar o valor das informações organizacionais, sua forma de classificação e sua importância para a continuidade do negócio. Numa visão da gestão da segurança da informação baseada no gerenciamento do risco, foram levantados os principais componentes do risco e as medidas de proteção adequadas, as ameaças ao negócio e as possíveis técnicas de defesa. Outros itens pesquisados na literatura foram as normas internacionais relativas à gestão da segurança da informação, seu histórico e seus itens de controles. Vários autores foram consultados sobre o uso de TI em pequenas empresas e gestão da segurança da informação, bem como os fatores de sucesso e insucesso para sua implementação e os influenciadores para sua adoção.

2.1 CONCEITO DE SEGURANÇA DA INFORMAÇÃO

Segurança da informação é um tema atual em constante discussão nas mais diversas organizações, seja governo, educação, indústria, comércio ou serviços; visto que as organizações utilizam-se da TI para apoiar e gerar negócios, aliados aos benefícios da Internet. Desse modo, independentemente do segmento de mercado, *core business* ou porte, todas as organizações sempre usufruirão da informação, objetivando melhor produtividade, redução de custos, ganho na participação de mercado, aumento de agilidade, competitividade e apoio à tomada de decisão. (SÊMOLA, 2003, p. 1).

Segurança da informação, conforme Beal (2005), é o processo de proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade. Sêmola (2003) define segurança da informação como “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.” A ISO/IEC 17799:2005, em sua seção introdutória define segurança da informação como “a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de

negócio”. Assim, podemos definir segurança da informação como a área do conhecimento que visa à proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade a fim de garantir a continuidade do negócio e minimizar os riscos.

Beal (2005) e Sêmola (2003) asseveram que o objetivo da segurança da informação é preservar os ativos de informação quanto a sua confidencialidade, integridade e disponibilidade:

- a **confidencialidade** da informação é a garantia de que somente pessoas autorizadas terão acesso a ela, protegendo-a de acordo com o grau de sigilo do se conteúdo;
- a **integridade** da informação tem como objetivo garantir a exatidão da informação, assegurando que pessoas não autorizadas possam modificá-la, adicioná-la ou removê-la, seja de forma intencional ou acidental;
- a **disponibilidade** garante que os autorizados a acessarem a informação possam fazê-lo sempre que necessário.

Sêmola (2003) ainda acrescenta a estes três objetivos o de:

- **legalidade** - garantia de que a informação foi produzida em conformidade com a lei;
- **autenticidade** - garantia de que num processo de comunicação os remetentes sejam exatamente o que dizem ser e que a mensagem ou informação não foi alterada após o seu envio ou validação.

Para Beal (2005), o objetivo *legalidade* é melhor classificado como objetivo organizacional, assim como o objetivo de *uso legítimo da informação* citados por outros autores, pois deles derivam os requisitos de segurança da informação. Quanto ao objetivo: *autenticidade*, a autora o entende necessário somente quando usado num processo de transmissão de informações, e estabelece alguns objetivos adicionais relativos à segurança da comunicação:

- integridade do conteúdo;
- irretratabilidade da comunicação;

- autenticidade do emissor e do receptor;
- confidencialidade do conteúdo;
- capacidade de recuperação do conteúdo pelo receptor.

Sêmola (2003) adverte sobre a expressão “Segurança da Informação”, dizendo que por si só, é um termo ambíguo, podendo assumir dupla interpretação: segurança como uma prática adotada para tornar um ambiente seguro ou o resultado da prática adotada, objetivo a ser alcançado. O autor cita exemplos:

- **segurança como “meio”** – a segurança da informação visa garantir a confidencialidade, integridade e disponibilidade da informação, a impossibilidade de agentes participantes em transações ou na comunicação repudiem a autoria de suas mensagens, a conformidade com a legislação vigente e a continuidade dos negócios;
- **segurança como “fim”** – a segurança da informação é alcançada por meio de práticas e políticas voltadas a uma adequada padronização operacional e gerencial dos ativos, e processos que manipulem e executem a informação.

Para Cernev e Leite (2005), deve-se tomar cuidado com a definição de segurança pela confusão corrente do termo com risco, privacidade e confiança. No caso da confiança explicam: “confiança engloba e significa muito mais do que segurança. Confiança é o pilar de sustentação de qualquer negócio ou empreendimento, tradicional ou eletrônico, dentro ou fora da Internet, sendo a segurança um dos seus principais construtos”.

Existem alguns termos relacionados à gestão da segurança da informação que merecem atenção; são eles (SÊMOLA, 2003; BEAL, 2005):

- **Ativo**: tudo aquilo que tem valor para a organização;
- **Ameaça:** expectativa de acontecimento acidental ou proposital, causado por um agente, que pode afetar um ambiente, sistema ou ativo de informação. É algo normalmente externo ao ativo que se quer proteger (falha de energia, fogo, vírus);

- **Vulnerabilidade:** fragilidade que poderia ser explorada por uma ameaça para concretizar um ataque. Está associada ao próprio ativo, podendo ser decorrente de uma série de fatores, como falta de treinamento, falta de manutenção, falha nos controles de acesso etc;
- **Impacto:** efeito ou conseqüência de um ataque ou incidente para a organização;
- **Ataque:** evento decorrente da exploração de uma vulnerabilidade por uma ameaça. Exemplos de ataque: digitação incorreta de dados pelo usuário, vazamento de informações, inclusão indevida no sistema de pagamento de compra fictícia;
- **Incidente:** fato (ou evento) decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades, levando à perda de princípios da segurança da informação: confidencialidade, integridade e disponibilidade.

2.1.1 IMPLEMENTAÇÃO DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Para se implementar a gestão da segurança da informação, Beal (2005) sugere o uso do método PDCA, muito utilizado em sistemas de gestão da qualidade. O significado da sigla PDCA vem de:

- P = *Plan*, de planejar
- D = *Do*, de executar
- C = *Check*, de verificar, avaliar
- A = *Act*, de agir corretivamente

Com o uso do método PDCA, a autora estipulou as seguintes etapas aplicadas à gestão da segurança da informação:

- Planejamento da segurança – começando do nível mais alto, identificam-se os processos críticos de negócio e dos fluxos de informação associados, para depois descer para o nível dos sistemas e serviços de informação e da infra-estrutura de TI que dá suporte a tais sistemas e serviços;

- Implementação da segurança – as atividades necessárias para se colocar em prática aquilo que foi planejado para atender aos requisitos de segurança da organização;
- Avaliação e ação corretiva – nesta etapa, deve-se coletar o maior número possível de informações e averiguar se a segurança implantada atende aos requisitos da fase de planejamento;
- Análise crítica independente da segurança da informação – recomenda que seja feito, por auditoria interna ou prestador de serviços especializado na área, um levantamento que ajude a garantir que as práticas da organização permaneçam condizentes com sua política e adequadas para situação de risco existente.

Quando se implementa um processo de gestão da segurança da informação, procura-se eliminar o máximo possível de pontos fracos ou garantir o máximo de segurança possível. (CARUSO e STEFFEN, 1999).

Conforme Beal (2005, p. XII) “os problemas de segurança da informação são complexos, e normalmente têm sua origem em preocupações organizacionais e de negócio, não de tecnologia.” A fim de garantir um nível de proteção adequado para seus ativos de informação, as organizações e seus principais gestores precisam ter uma visão clara das informações que estão tentando salvaguardar, de que ameaças e por que razão, antes de poder passar a seleção de soluções específicas de segurança. Grande parte dos dados importantes ao negócio da empresa está armazenada em computadores, por isso as organizações dependem da confiabilidade de seus sistemas baseados em TI; se a confiança nesses dados for destruída, o impacto pode ser comparável à própria destruição do sistema.

Ainda conforme a autora, os administradores devem preocupar-se com a segurança dos componentes de TI e da informação neles armazenada por quatro razões principais:

- Dependência da tecnologia da informação;
- Vulnerabilidade da infra-estrutura tecnológica – hardware e software;
- Alto valor da informação armazenada;

- Pouca atenção dada à segurança nos estágios iniciais do desenvolvimento de software.

Dessa forma, as organizações precisam adotar controles de segurança – medidas de proteção que abranjam uma grande diversidade de iniciativas – que sejam capazes de proteger adequadamente dados, informações e conhecimentos, escolhidos, levando-se em conta os riscos reais a que estão sujeitos esses ativos. (BEAL, 2005).

À medida que as empresas tornam-se mais dependentes da informática, mais vulneráveis ficam as organizações a crimes e fraudes cometidos com o uso de recursos computacionais. Na maioria dos casos ocorridos, nada é publicado, por necessidade de preservação da imagem. Porém em média, após a ocorrência de um desastre completo no departamento de TI, a capacidade de operação da empresa declina em 90% e segundo estatísticas mundiais, mais de 75% das empresas que sofrem esse tipo de desastre deixam de existir ou acabam sendo compradas. (CARUSO e STEFFEN, 1999).

Os autores ainda alertam que é importante que a segurança da informação não seja tratada como um segredo militar ou diplomático, mas não se deve deixá-la ao acaso, pois, mais cedo ou mais tarde, aparece alguém que não só conhece os meios técnicos para se apossar das informações, como sabe lucrar com elas.

2.1.2 INFORMAÇÕES RECENTES SOBRE SEGURANÇA DA INFORMAÇÃO

Informações recentes publicadas na mídia indicam o crescimento de incidentes de segurança da informação, suas principais ameaças e os investimentos na área:

- Dados divulgados pelo Comitê Gestor da Internet no Brasil através do Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.br) mostram que o número de incidentes de segurança motivados por falhas e vulnerabilidades de software a ataques externos, vírus etc, passou de 3,1 mil em 1999 para 52,6 mil em 2004. Houve, entre o final de 2002 e o

primeiro trimestre de 2003, um aumento de 84% no número de ataques e incidentes de segurança (MESQUITA, 2003).

- Uma pesquisa mais recente do CERT.br aponta um crescimento de 1.313% no segundo trimestre de 2005 nas notificações associadas às fraudes virtuais, se comparadas com o mesmo período de ano passado. “Em relação ao trimestre anterior, as fraudes cresceram 259%” (BANTEL, 2005).

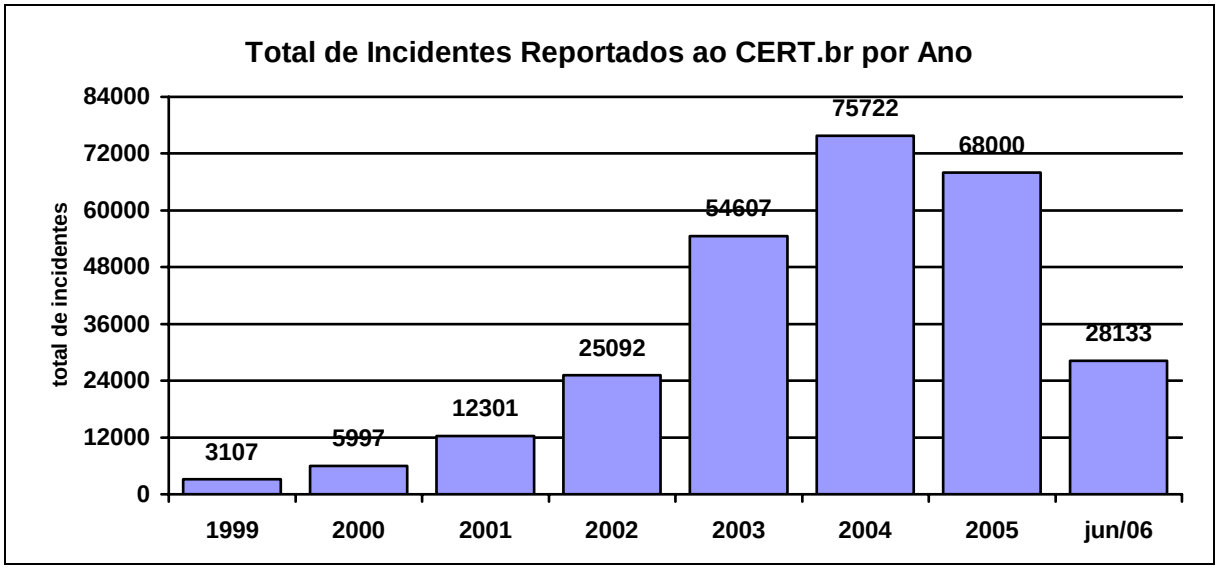

Gráfico 1: evolução dos ataques externos reportados no Brasil
Fonte: Comitê Gestor da Internet no Brasil (2006)

- Outro estudo do Comitê Gestor da Internet no Brasil (2006) destaca que praticamente metade das empresas brasileiras com acesso à Internet já sofreu algum incidente de segurança, sendo o mais comum o ataque de vírus (50%), seguido pelo ataque de *trojans* (31%) e pelos *worms* ou *bots* (17%). A pesquisa também revela que as empresas têm consciência do problema e utilizam as seguintes medidas de proteção: 96% usam antivírus, 60% utilizam software *anti-spyware*, 54% possuem *firewall* e 49% usam conexão segura entre clientes e servidores (via SSL, HTTPS).

- Segundo ComputerWorld (2006), as pequenas e médias empresas brasileiras deverão investir em 2007 cerca de 260 milhões de dólares com soluções de segurança em TI, em virtude, principalmente, da ascensão dos crimes digitais. Os investimentos em aplicações de *firewall* e antivírus continuam, porém serão feitos investimentos com maior intensidade em soluções de Redes Privadas Virtuais (*Virtual Private Network* - VPN) e *softwares* de

detecção ou prevenção de intrusões. Segundo o estudo, cerca de 50% das médias empresas do País implantaram um roteador ou uma aplicação baseada em firewall em suas operações. Ao mesmo tempo, 24% delas pretendem implementar algo desse tipo nos próximos 12 meses.

- A 9ª Pesquisa Nacional de Segurança da Informação (Módulo, 2003) constatou que 23% dos entrevistados vêem a falta de consciência dos executivos como o principal obstáculo para implementação da segurança, em contrapartida a outros fatores como: dificuldade de demonstrar o retorno, custo, falta de consciência dos usuários, falta de prioridade, falta de orçamento, entre outros.

2.2 O VALOR DAS INFORMAÇÕES

O bem mais valioso de uma empresa são as informações relacionadas com os bens de consumo ou serviços prestados por ela (CARUSO e STEFFEN, 1999), e pela alta capacidade que dados, informação e conhecimento têm de adicionar valor a processos, produtos e serviços, esses constituem recursos cada vez mais críticos para o alcance da missão e dos objetivos organizacionais. Conseqüentemente, as informações críticas para o negócio precisam ser protegidas contra as ameaças que podem levar à sua destruição, indisponibilidade temporária, adulteração ou divulgação não autorizada. (BEAL, 2005, p. XI).

“A informação é um recurso que tem valor para a organização e deve ser bem gerenciada e utilizada [...] é necessário garantir que ela esteja sendo disponibilizada apenas para as pessoas que precisam dela para o desempenho de suas atividades profissionais”. (FONTES, 2006, p. 38). O autor ainda alerta que o maior risco para as informações é a organização não se preocupar com a segurança e com os possíveis ataques a ela, achando que isso acontece apenas com os outros.

“É importante que os gestores se conscientizem de que todas as informações têm algum tipo de valor para alguém e/ou para algo; o que ocorre é que ainda não se descobriu para quem ou para quê.” (CARUSO e STEFFEN, 1999).

> O ser humano sempre buscou o controle sobre as informações que lhe eram importantes, até mesmo na mais remota antiguidade, o que mudou foram as formas de registro e armazenamento dessas informações, que nos dois últimos séculos passaram a ter importância crucial para as organizações humanas. Devido ao modo arcaico de registro de informações na antiguidade, era natural que o controle e disseminação das informações tornassem o acesso às mesmas restrito e a uma minoria sempre ligada ao grupo que dominava o poder econômico e político da sociedade. Os primeiros suportes para registro de informações foram as paredes das habitações humanas; por si só implicava um conjunto de conseqüências: restrições de acesso físico, de transferências para terceiros ou para outro local e de pessoal capacitado. Além da "imobilidade" das informações, quase ninguém na época detinha conhecimento necessário para reconhecê-las. Em meados do século XX a alfabetização se universalizou, o que possibilitou a várias pessoas o acesso à informação. (CARUSO e STEFFEN, 1999).

Para os autores, "não há organização humana que não seja dependente da tecnologia de informações", fato que se potencializou em função da evolução da informática com o acúmulo de grande quantidade de informações em pequenos espaços. Essa característica acarreta conseqüências graves para essas mesmas organizações, por facilitar os ataques de pessoas não-autorizadas. Independente do setor da economia em que a empresa atue, as informações estão relacionadas com seus processos de produção e de negócios, políticas estratégicas, de marketing, cadastros de clientes, dados contábeis e financeiros etc. E não importa o meio de armazenamento, elas são de valor inestimável não só para a empresa que as gerou como também para seus concorrentes.

Segundo Moraes, Terence e Escrivão Filho (2004), nenhuma empresa pode escapar aos efeitos da revolução causada pela informação; dessa forma, deve-se ter consciência de que a informação é um requisito tão importante quanto os recursos humanos, pois dela depende o sucesso ou fracasso das tomadas de decisões diárias.

Os riscos são agravados, à medida que informações essenciais aos negócios da empresa são centralizadas. Ainda que esses riscos sejam sérios, as vantagens dessa centralização são maiores, tanto sob aspectos econômicos como pela agilização de processos na tomada de decisão.

Segurança, mais que estrutura hierárquica, homens e equipamentos, envolve uma postura gerencial, o que ultrapassa a tradicional abordagem da maioria das empresas. É preciso cercar o ambiente de informações com medidas que garantam sua segurança efetiva, a um custo aceitável, visto ser impossível obter-se segurança

absoluta, já que a partir de um determinado ponto, os custos se tornam inaceitáveis. (CARUSO e STEFFEN, 1999).

2.3 GERENCIAMENTO DO RISCO

A segurança de informações confidenciais para a empresa sempre foi de extrema importância. Tanto informações armazenadas em papel quanto informações armazenadas em banco de dados computacionais, na mão de pessoas erradas podem trazer prejuízos dos mais variados possíveis para as empresas. A estrutura da segurança de informações não pode ser algo estático dentro da empresa e depende da cooperação de todos os envolvidos para seu sucesso. Porém muitos gestores têm ignorado os riscos que os seus negócios correm com o vazamento e perda de informações e simplesmente não se preocupam o suficiente com a segurança da informação. (CARUSO e STEFFEN, 1999).

Dessa forma, “toda a organização precisa adquirir uma visão sistêmica das suas necessidades de segurança, dos recursos a serem protegidos e das ameaças às quais está sujeita, para então poder identificar as medidas de proteção mais adequadas, economicamente viáveis e capazes de reduzir ou eliminar os principais riscos para o negócio.” (BEAL, 2005).

Fontes (2006) alerta para o constante crescimento de incidentes de segurança da informação, principalmente no Brasil. De forma crescente as organizações estão potencialmente mais expostas a novas formas de ataques, independentemente do porte ou do tipo de negócio.

Devido à alta complexidade e ao alto custo de manter os ativos da informação salvos de ameaças à sua confidencialidade, integridade e disponibilidade, é importante adotar um enfoque de gestão baseado nos riscos específicos para o negócio. (Beal, 2005).

O risco é a probabilidade de ocorrência de um evento adverso para uma determinada situação esperada. Sêmola (2003) o define como: “a probabilidade de que agentes, que são ameaças, explorem vulnerabilidades, expondo os ativos a perdas de confidencialidade, integridade e disponibilidade, e causando impacto nos negócios”. Os impactos são limitados por medidas de segurança, que ajudam a

diminuir o risco. Para demonstrar essa relação, o autor propõe a seguinte equação do risco de segurança da informação:

$$\text{RISCO} = \frac{\text{VULNERABILIDADES x AMEAÇAS x IMPACTOS}}{\text{MEDIDAS DE SEGURANÇA}}$$

Para Hitt (2005), a gestão do risco é estratégica, pois influencia diretamente as capacidades e competências essenciais da empresa, com maior ênfase nos riscos administrativo e individual. Os riscos interagem com a realidade e são fatos na vida corporativa, uma vez que resultados incertos são reflexos de decisões gerenciais.

> Gestão do risco é o conjunto de processos que permite às organizações identificar e implementar as medidas de proteção necessárias para diminuir os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos. (BEAL, 2005).

A figura 1 exibe os componentes do risco e as principais medidas de proteção usadas para reduzi-lo:

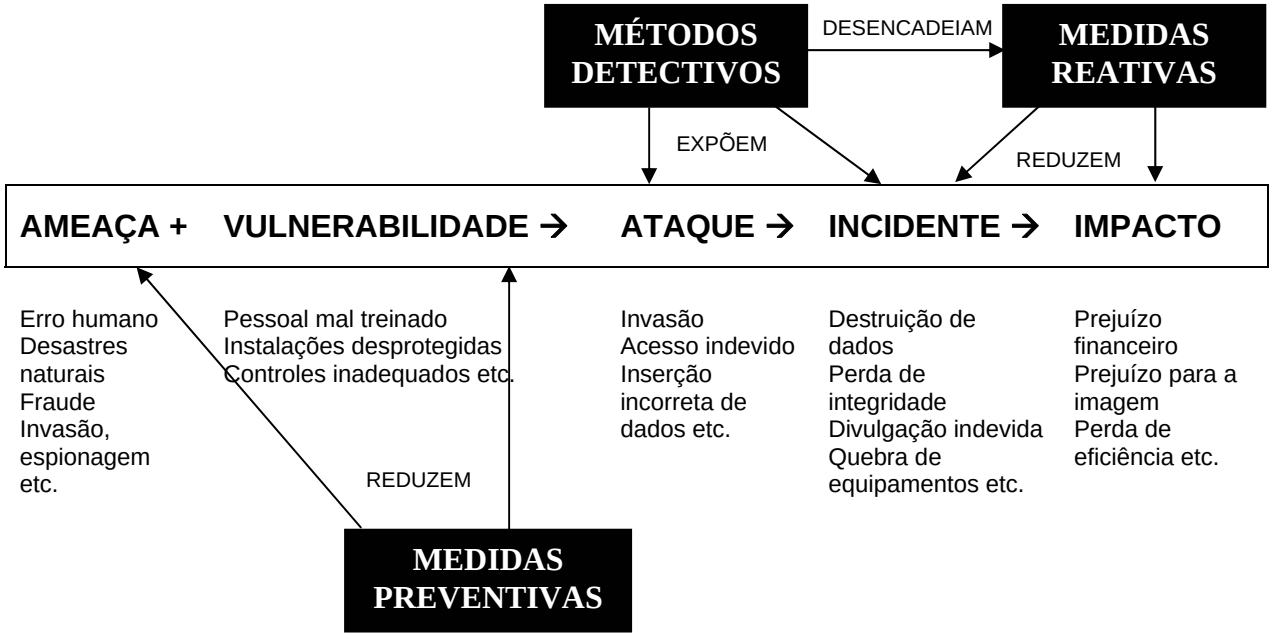

Figura 1: componentes do risco e medidas de proteção usadas para reduzi-lo.
Fonte: Beal (2005).

As ameaças somadas às vulnerabilidades quando mal gerenciadas facilitam o ataque a um ativo da informação. Um ataque concluído gera o incidente de segurança que culmina em um impacto para os negócios da organização. As seguintes medidas podem ser implementadas para melhor gerenciar o risco:

- MEDIDAS PREVENTIVAS: reduzem a probabilidade de uma ameaça se concretizar ou diminuem o grau de vulnerabilidade do ambiente, ativo ou sistema; reduzindo assim a probabilidade de um ataque e/ou sua capacidade de gerar efeitos adversos na organização. Exemplos de medidas preventivas:
    - Política de segurança;
    - Controles de acesso físicos e lógicos;
    - Programas de conscientização e treinamento; etc.
- MÉTODOS DETECTIVOS: expõem ataques ou incidentes e disparam medidas reativas, tentando evitar a concretização do dano, reduzi-lo ou impedir que se repita. Exemplos de métodos detectivos:
    - Monitoração da rede;
    - Sistemas de detecção de intrusos;
    - Auditorias; etc.
- MEDIDAS REATIVAS: reduzem o impacto de um ataque ou incidente. São medidas tomadas durante ou após a ocorrência do evento. Exemplos de medidas reativas:
    - Ação legal;
    - Restauração do serviço;
    - Procedimentos de resposta a incidentes; etc.

2.3.1 AMEAÇAS

> A todo instante os negócios, seus processos e ativos físicos, tecnológicos e humanos são alvo de investidas de ameaças de toda ordem, que buscam identificar um ponto fraco compatível, uma vulnerabilidade capaz de potencializar sua ação. Quando essa possibilidade aparece, a quebra de segurança é consumada. (SÊMOLA, 2001, p. 18).

"As ameaças do mundo digital espelham as ameaças no mundo físico. Se o desfalque é uma ameaça, então o desfalque digital também é uma ameaça. Se os bancos físicos são roubados, então os bancos digitais serão roubados." (SCHNEIER, 2001). O crime no ciberespaço inclui tudo o que se pode esperar do

mundo físico: roubo, extorsão, vandalismo, voyeurismo, exploração, jogos de trapaças, fraude, etc.

Desde que os computadores começaram a ser usados, as tentativas de acesso não autorizado a eles existem; entretanto, foi só após o uso comercial da Internet que o problema tornou-se mais crítico. Associados a essas ameaças encontram-se alguns termos que se tornaram manchetes de publicações destinadas ao público especializado em informática e até na imprensa não-especializada: (CARUSO e STEFFEN, 1999).

- ***Hackers*** – são em geral jovens e adolescentes, amadores aficionados por informática, normalmente com alto grau de inteligência e capacitação no ramo, cuja principal diversão é conseguir ultrapassar as barreiras de acesso aos grandes sistemas de computação que operam em rede, principalmente na Internet. Em uma outra definição, *hacker* é o indivíduo que conhece muito sobre tecnologia mas que não usa seus conhecimentos para o mal, enquanto que o termo *cracker*, define o aficionado por tecnologia que usa seus conhecimentos para praticar violações de sistemas e roubo de informações, de forma a obter proveito próprio ou para terceiros.

- ***Vírus*** – são programas de computador capazes de se reproduzir, se auto-copiando para disquetes, unidades de redes ou anexos de e-mail. Geralmente, destroem os programas e arquivos de seu computador, ou simplesmente o atrapalham deixando seu micro mais lento.

- ***Worm –*** é uma subclasse de vírus que geralmente se alastra sem a ação do usuário e distribui cópias completas de si mesmo através das redes. Um *worm* pode consumir memória e largura de banda de rede, o que pode travar o computador.

- **Cavalo de Tróia** – deve seu nome ao fato de funcionar baseado em estratégia similar contada pela mitologia grega. Atualmente o cavalo virou um programa e a Tróia um computador. Conhecidos também como *Trojan Houses*, estes programas são construídos de tal maneira que, uma vez instalados nos computadores, abrem “portas” no computador infectado, tornando possível o acesso de *hackers*.

- ***Backdoors*** – existe uma confusão entre o que é um *backdoor* e um *trojan*, principalmente porque os problemas provocados por ambos são semelhantes. Um *trojan* é um programa que cria deliberadamente um *backdoor* em seu computador. Eles são abertos devido a defeitos de fabricação ou falhas no projeto, isto pode acontecer tanto acidentalmente como propositalmente.

- **SPAM** – é o envio em massa de mensagens de e-mails não-solicitadas, algumas inofensivas, outras com conteúdo publicitário, porém, alguns invasores utilizam-se de SPAM para distribuição de códigos maliciosos.

- ***Spyware*** – é um programa instalado no computador do usuário sem seu consentimento que captura informações através de tudo que é digitado no teclado, seus costumes na Internet e informações pessoais para depois enviar a uma entidade externa na Internet. Podem ser desenvolvidos por empresas que desejam monitorar os hábitos do usuário e depois vendê-los na Internet.

Outra ameaça muito freqüente e que não depende necessariamente de recursos de TI é a engenharia social. Engenharia Social é a técnica de aproveitar-se da boa fé das pessoas para obter informações que possibilitem ou facilitem o acesso aos recursos computacionais de uma organização por parte de usuários não autorizados. Fontes (2006) define engenharia social como: “o conjunto de procedimentos e ações que são utilizados para adquirir informações de uma organização ou de uma pessoa por meio de contatos falsos sem o uso da força, do arrombamento físico ou de qualquer brutalidade”. Mitnick e Simons (2003) definem a engenharia social como a arte de fazer com que as pessoas façam coisas que normalmente não fariam para um estranho.

Existem diversas formas de se efetuar um ataque de engenharia social, mas todas elas têm em comum a característica de usarem basicamente psicologia e perspicácia para atingir os seus propósitos. Atualmente, as mais populares são:

- Usar telefone ou e-mail para se fazer passar por uma pessoa ou instituição que precisa de determinadas informações para resolver um suposto problema;

- Enviar programas maliciosos ou instruções especialmente preparadas, com o objetivo de abrir brechas na segurança da rede ou coletar o máximo de informações possíveis sobre ela. Essa técnica ficou conhecida como ***Phishing***, pois leva a vítima até uma página falsa na Internet, que pode instalar um *trojan* no computador da vítima. Em outros casos pode ser de uma instituição financeira, com a qual geralmente a vítima possui relacionamento, fazendo que forneça seus dados como agência, conta e senha, para depois efetuar fraudes eletrônicas. Também conhecido como *Phishing Scam* ou somente *Scam*.

A principal maneira de se prevenir contra estes ataques é orientando os usuários e administradores de redes e sistemas sobre como agir nestas situações. Procure reduzir a exposição da rede em fóruns públicos na Internet e não revele nada mais que o suficiente sobre a topologia da rede. Tome cuidado com orientações passadas por pessoas desconhecidas, e evite executar programas de origem obscura ou não confiável – eles podem ser uma armadilha.

2.3.2 TÉCNICAS DE DEFESA

O que se pode fazer está relacionado com diversas técnicas e pacotes que cuidam de aspectos diversos do problema e que podem ser usados para essa finalidade, como, por exemplo:

- **Política de Segurança** - é um instrumento importante para proteger as empresas contra ameaças à segurança da informação. Ela não define procedimentos específicos de manipulação e proteção da informação, mas atribui direitos e responsabilidades aos usuários (funcionários, gerentes, administradores de redes e sistemas, etc) que lidam com essa informação. A política de segurança também estipula as penalidades às quais estão sujeitos os que a descumprem;

- **Plano de Contingência** - consiste em procedimentos de recuperação preestabelecidos, com a finalidade de minimizar o impacto sobre as atividades da organização, no caso de ocorrência de um dano ou desastre que os procedimentos de segurança não conseguiram evitar;

- **Softwares de Segurança e *Firewall*** - um *firewall* é uma barreira inteligente entre a sua rede local e a Internet, através da qual só passa tráfego autorizado. Este tráfego é examinado pelo *firewall* em tempo real e a seleção é feita de acordo com a regra "o que não foi expressamente permitido, é proibido".

- **Sistema de *Backup*** - corresponde a cópias de segurança de todas as informações importantes para a empresa que reside em seus servidores e microcomputadores. Nunca deve ser feito dentro da própria máquina, e mesmo sendo feito em mídia removível, é extremamente aconselhável que essa fique guardada em local seguro, de preferência fora do perímetro da empresa. O *backup* é feito geralmente de madrugada, quando ninguém está utilizando o sistema.

- **Software Antivírus** – são programas destinados a barrar e combater os vírus de computadores; os mais recentes incluem proteção contra *worms*, *trojans* e *spywares*.

- **Atualizações do sistema operacional e aplicativos** – várias vulnerabilidades são descobertas em programas de uso diário como o sistema operacional (Windows, Linux) e programas aplicativos (Word, Excel, PowerPoint etc). Mantê-los atualizados com as mais recentes correções contribui para minimizar os riscos de um incidente em segurança da informação.

Para Caruso e Steffen (1999), toda rede local com conexão dedicada à Internet precisa de proteção. É um engano pensar que somente as grandes corporações são alvo de *hackers*. Qualquer empresa com conexão dedicada à Internet é um alvo, pois as ferramentas automáticas de *hackers* atacam milhares de endereços por hora e invadem o primeiro site desprotegido. Segundo os autores existem mais de 80.000 *sites* na própria Internet dedicados a atividades de *hacking* onde é possível obter ferramentas para invasão de sistemas.

Entretanto, nenhum dos recursos acima resolve todos os problemas de ataques. Esse tipo de tarefa deve ser feito mais no campo administrativo, com medidas destinadas a disciplinar o uso de recursos, como: senhas individuais e secretas, auditoria das atividades executadas na rede, documentação organizada,

evitar ao máximo o acúmulo de responsabilidades e funções nas mãos de poucas pessoas. Ressalta-se que, independentemente da forma de controle de acesso adotada, não existem meios de se impedir que uma pessoa autorizada e com o nível de acesso suficiente cause danos, de forma voluntária ou não. (CARUSO e STEFFEN, 1999).

Fontes (2006) assevera que “a classificação e uma política rígida de utilização da informação são medidas preventivas que podem ajudar a minimizar os riscos”. Mitnick e Simon (2003, p. 210) corroboram ao afirmarem que “uma política de classificação de dados é fundamental para proteger as informações de uma organização e estabelecer as categorias responsáveis pela liberação das informações confidenciais”. Na visão de Beal (2005) inventariar os ativos da informação existentes e classificá-los de acordo com o valor e o grau de sensibilidade atribuída pela organização permite determinar mais precisamente os requisitos de tratamento e proteção a eles aplicáveis.

Os autores Mitnick e Simon (2003) sugerem a classificação das informações em:

- **Confidencial** – informações compartilhadas com um número muito limitado de pessoas que tenham necessidade absoluta de conhecê-las;
- **Particular** – informações de natureza pessoal que se destinam apenas ao uso dentro da organização, como: histórico médico de empregados, os benefícios de saúde, histórico de salário etc.;
- **Interna** – informações que podem ser fornecidas livremente para todos os empregados da organização, mas que devem ser controladas para vazamento externos e de terceiros. Exemplo: gráficos organizacionais, nomes dos sistemas internos, procedimentos de acesso remoto etc.;
- **Pública** – informações criadas especificamente para liberação ao público, como: telefone do serviço de atendimento ao cliente (SAC), manuais do produto, notícias para a imprensa etc.

Grande parte dos problemas de segurança são originados na rede interna da organização e, muitas vezes, são causados pelo desconhecimento de conceitos e procedimentos básicos de segurança por parte dos usuários. Um exemplo deste

problema é a má configuração do programa de leitura de e-mails de um usuário, que faz com que qualquer arquivo anexado a uma mensagem seja automaticamente aberto ou executado, permitindo a instalação de *backdoors*, cavalos de tróia, disseminação de vírus etc.

Um fator que contribui para o processo de educação dos usuários é o estabelecimento de políticas de segurança claras, conhecidas e completamente entendidas pelos usuários da rede. O estabelecimento de um canal de comunicação (intranet, lista de e-mail, cartazes etc.) para transmitir informações importantes sobre segurança de informações e principalmente a notificação de descoberta de um novo vírus, sua forma de infecção e métodos de prevenção.

Porém, o uso de treinamentos periódicos não deve ser descartado, podem ser treinamentos curtos de duas ou quatro horas de maneira a sensibilizar o usuário para o uso correto dos ativos de informação da organização.

2.4 CAMADAS DE SEGURANÇA DA INFORMAÇÃO

Para facilitar o entendimento e o estudo da gestão da segurança em Internet *Banking*, Adachi (2004) utilizou em sua dissertação de mestrado uma classificação em três camadas da segurança da informação: física, lógica e humana. Este trabalho usa esta classificação, vislumbrando um modo mais amplo que o tratado pela autora, ao estudar todo o processo de gestão da segurança da informação e não somente a segurança do Internet *Banking*.

Segue a definição das três camadas de segurança da informação:

- **Camada física** – é o ambiente onde está instalado fisicamente o *hardware* – computadores, servidores, meio de comunicação – podendo ser o escritório da empresa, a fábrica ou até a residência do usuário no caso de acesso remoto ou uso de computadores portáteis. O controle de acesso aos recursos de TI, equipamentos para fornecimento ininterrupto de energia e *firewalls* são algumas das formas de gerir a segurança desta camada.
- **Camada lógica** - é caracterizada pelo uso de *softwares* - programas de computador - responsáveis pela funcionalidade do *hardware*, pela realização

de transações em base de dados organizacionais, criptografia de senhas e mensagens etc. As atualizações de segurança, disponibilizadas pelos fabricantes, contra vulnerabilidades conhecidas representam uma das formas de controlar a segurança desta camada.

- **Camada humana** - é formada por todos os recursos humanos presentes na organização, principalmente os que possuem acesso a recursos de TI, seja para manutenção ou uso. São aspectos importantes desta camada: a percepção do risco pelas pessoas: como elas lidam com os incidentes de segurança que ocorrem; são usuários instruídos ou ignorantes no uso da TI; o perigo dos intrusos maliciosos ou ingênuos; e a engenharia social (ADACHI, 2004). A política de segurança e a conscientização dos usuários são algumas das formas de controlar a segurança desta camada.

> A gestão destas camadas pode ser feita de diversas formas: centralizada, por camada e especialidade; interdisciplinar, que atinge mais de uma camada e por processos, que permeiam um item como cadastramento de usuário e acesso final. A idéia central da divisão por camadas é categorizar os temas, ou domínios a serem abordados, em uma gestão de segurança. (ADACHI, 2004, p. 78)

> Com uma só camada de defesa, os ativos da informação passam a estar vulneráveis assim que um ataque consegue superar esse nível único de proteção. [...] Uma boa “segurança em camadas” abrange controles físicos, lógicos e manuais, e considera o equilíbrio entre medidas de prevenção, detecção e recuperação de possíveis impactos. (BEAL, 2003, p. 168)

Sêmola (2003) classifica a gestão da segurança da informação dividindo-a em três aspectos: tecnológicos, físicos e humanos. Para o autor as organizações preocupam-se principalmente com os aspectos tecnológicos (redes, computadores, vírus, *hackers*, Internet) e se esquecem dos outros – físicos e humanos – tão importantes e relevantes para a segurança do negócio quanto os aspectos tecnológicos.

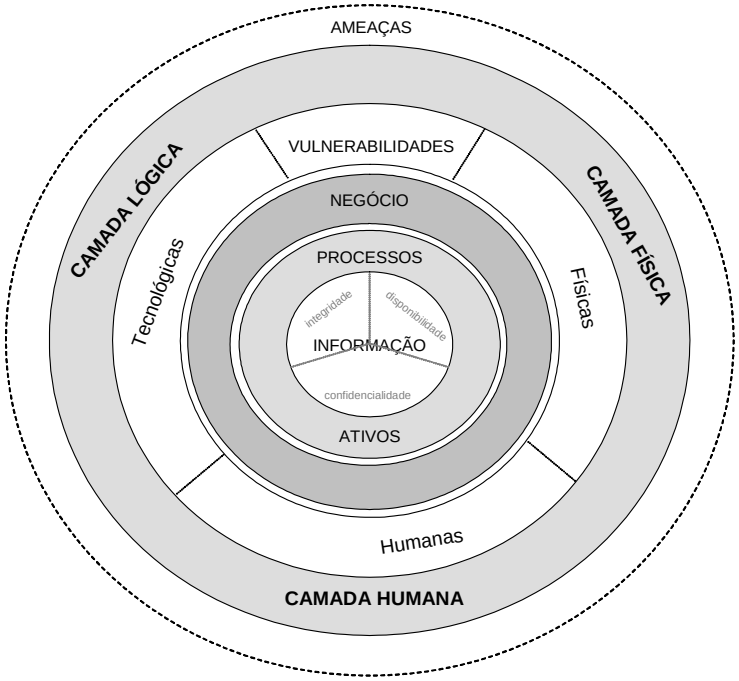

Figura 2: escopo da solução de segurança da informação em camadas.
Fonte: adaptado de Sêmola (2005).

2.4.1 CAMADA FÍSICA

> A camada física representa o ambiente em que se encontram os computadores e seus periféricos, bem como a rede de telecomunicação com seus modems, cabos e a memória física, armazenada em disquetes, fitas ou CDs. (ADACHI, 2004).
>
> A segurança física relaciona-se diretamente com os aspectos associados ao acesso físico a recursos de informações, tais como disponibilidade física ou o próprio acesso físico, sejam esses recursos as próprias informações, seus meios de suporte e armazenamento ou os mecanismos de controle de acesso às informações. Além disso, está também relacionada com as técnicas de preservação e recuperação das informações e seus meios de suporte e armazenamento. (CARUSO e STEFFEN, 1999)

No caso de informações, o acesso físico está representado pelo acesso ao meio de registro ou suporte que abriga as informações. No caso de informações registradas em papel, não há como separar o acesso físico do lógico.

O acesso físico está muito menos sujeito a riscos do que o acesso lógico, entretanto, o controle pode ser mais difícil, já que depende muito mais de intervenção humana.

Normalmente, os riscos relacionados com o acesso físico afetam os meios de registro e suporte das informações, ao passo que os riscos relacionados com o acesso lógico afetam o conteúdo.

Os controles importantes de segurança desta camada, são:

- Prevenir acesso físico não-autorizado às instalações;
- Proteção de acesso à sala dos servidores, somente para pessoal autorizado;
- Controle de acesso a visitantes;
- Prevenção contra incêndio;
- Proteção e controle de acesso físico aos servidores;
- Prevenção contra quedas de energia.

2.4.2 CAMADA LÓGICA

A camada lógica é composta por programas e aplicativos – *softwares*. Segundo Adachi (2004), é nessa camada que estão as “regras, normas, protocolo de comunicação e onde efetivamente, ocorrem as transações e consultas.”

A segurança de acesso lógico refere-se ao acesso que indivíduos têm a aplicações residentes em ambientes informatizados, não importando o tipo de aplicação ou o tamanho do computador. As ferramentas de controle são, em sua maior parte, “invisíveis” aos olhos de pessoas externas aos ambientes de informática; estas só os reconhecem quando têm o seu acesso barrado pelo controle de acesso.

O mecanismo básico de controle de acesso lógico era inicialmente baseado em senhas. Entretanto, as senhas são um mecanismo muito frágil e, atualmente, seu papel resume-se mais em autenticar a identidade de usuários que estão tentando acessar determinado ambiente protegido. O acesso propriamente dito é controlado por mecanismos de listas de acesso, que descrevem quais usuários podem acessar quais recursos e, dentro de cada recurso que o mesmo tenha direito de acessar, qual o nível de acesso concedido. O controle de acesso lógico está relacionado com as atividades de controle e auditoria normalmente existentes dentro das maiores organizações.

> O termo acesso lógico, comumente usado em informática, de forma precisa é o “acesso ao ambiente de informações”. Está relacionado com o acesso ao conteúdo informacional. Faz mais sentido para acesso a ambientes informatizados, que são colocados à disposição de pessoas para que executem as tarefas para as quais foram contratadas. Ele abrange aspectos como o acesso de pessoas a terminais e outros equipamentos de computação e manuseio de listagem (parcialmente uma questão de acesso físico), funções autorizadas dentro do ambiente informatizado, a exemplo de transações que possam efetuar, arquivos aos quais tenham acesso, programas que possam executar, etc. Parte do acesso lógico se confunde com o acesso físico, sendo impossível separar onde começa um e onde termina o outro, a exemplo do acesso a equipamentos ou papéis. (CARUSO e STEFFEN, 1999)

A pequena e média empresa têm seus dados armazenados geralmente em servidores de rede ou em estações compartilhadas, onde nem sempre o acesso físico é restrito. Na maioria das vezes, esse mesmo servidor ou estação possui acesso liberado e ilimitado a Internet, o que aumenta o risco de um incidente de segurança. Como as pequenas empresas possuem menos recursos financeiros e humanos do que grandes empresas, o controle de acesso a esses recursos é negligenciado: as senhas de acesso são compartilhadas entre todos os empregados, não existe classificação de informação e nem termo de utilização de recursos de TI. Na média empresa, o cenário é menos problemático, porém não o ideal, principalmente devido à conscientização dos funcionários sobre segurança da informação.

> O que antes era realizado por pessoas, foi migrado para as máquinas (*hardwares*), que pensam conforme foram programadas (*softwares*), portanto, a camada lógica está sempre sendo ameaçada e é um dos pontos focais para ataques. Os ataques, à distância, ocorrem na camada lógica, por meio de vírus, cavalos-de-tróia e e-mails maliciosos. (ADACHI, 2004)

Nesta camada, conforme o guia desenvolvido pela Interpol sobre segurança e métodos de prevenção de crimes de TI (INTERPOL, 2000) apud ADACHI (2004), podem ser implantadas as seguintes medidas de precauções no servidor:

- Registro (*log*) de quem, quando, o que e onde foi realizado um evento (este dado é o material mais importante em uma investigação);
- *Backup* dos dados e redundância dos sistemas e aplicativos;
- *Firewall* para filtrar as informações que entram e saem;
- Sistema para detectar intrusão nos sistemas e programas.

Do outro lado, as estações se previne das seguintes formas:

- Instalar e atualizar, constantemente, o sistema de *firewall* pessoal e de antivírus;
- Manter atualizado os aplicativos com as correções (*patches*) sugeridas pelos fornecedores idôneos de softwares;
- Não instalar no computador programas suspeitos.

2.4.3 CAMADA HUMANA

Das três camadas, esta é a mais difícil de se avaliarem os riscos e gerenciar a segurança, pois envolve o fator humano, com características psicológicas, sócio-culturais e emocionais, que variam de forma individual (SCHNEIER, 2001).

A gestão da segurança da informação envolve mais do que gerenciar os recursos de tecnologia – *hardware* e *software* – envolve pessoas e processos, porém algumas empresas negligenciam esse fator.

> Muitas tarefas humanas, realizadas por pessoas, estão sendo, cada vez mais, substituídas por máquinas, *softwares* e *hardwares*, isto ocorre por interesse relacionado à economia de custos, ganho em escala, necessidade de gerenciamento e também para minimizar os riscos de erros ou falhas humanas. Todavia, em todos os processos, sempre haverá um recurso humano, podendo ser desde o criador até o usuário final. (ADACHI, 2004)

Wadlow (2000) apud Adachi (2004) descreveu três qualidades que podem levar uma pessoa a atacar um sistema: habilidade, motivação e oportunidade. Os funcionários da empresa possuem duas das três qualidades: habilidade e oportunidade, basta ter uma motivação para ameaçar, invadir, fraudar ou roubar, quebrando a segurança da empresa. Desta forma, o processo e as condições de contratação de recursos humanos, internos ou externos, devem ser rigorosos, seguindo a política de segurança elaborada pela empresa. Uma política de segurança clara, largamente disseminada e incutida em todos os recursos humanos, é importante para zelar pela segurança da empresa e de seus clientes. Além disso, é importante que na política de segurança sejam discriminadas as penalidades, conforme as infrações, e que elas sejam efetivamente executadas, conforme julgamento de um conselho de análise de incidentes.

2.5 NORMAS E PADRÕES DE SEGURANÇA

“Normas e padrões têm por objetivo definir regras, princípios e critérios, registrar as melhores práticas e prover uniformidade e qualidade a processos, produtos ou serviços, tendo em vista sua eficiência e eficácia.” (BEAL, 2005, p. 36). Concomitantemente Sêmola (2003) diz “que uma norma tem o propósito de definir regras, padrões e instrumentos de controle que dêem uniformidade a um processo, produto ou serviço.”

Os principais padrões e normas seguidos atualmente pelas empresas são o COBIT e a ISO 17799.

2.5.1 COBIT

O *Control Objectives for Information and related Technology* (COBIT) é um guia formulado como *framework*, dirigido para a gestão de TI. Segundo Rocha (2003), “esse tradicional conjunto de boas práticas para o gerenciamento de processos traduz a realidade da governança em TI de uma organização.”

> O COBIT provê boas práticas para o gerenciamento dos processos de TI em uma estrutura lógica e gerenciável, encontrando as múltiplas necessidades do gerenciamento empresarial, interligando os *gaps* entre os riscos de negócio, assuntos técnicos, necessidades de controle e requisitos de medições de performance. O COBIT habilita o desenvolvimento de uma política clara e de boas práticas para o controle de TI da organização, dentre eles possui amplas recomendações de segurança da informação. O COBIT é bastante usado no Brasil pela comunidade de auditoria, em especial no segmento bancário. (NERY e PARANHOS, 2003)

2.5.2 ABNT NBR ISO/IEC 17799:2005

A fim de implementar e normalizar a atuação das empresas na gestão da segurança da informação, em 1989, o *Commercial Computer Security Center*, órgão ligado ao departamento de indústria e comércio do Reino Unido, publicou a primeira versão do Código para Gerenciamento de Segurança da Informação - PD0003. Seis anos depois, este código foi revisado e publicado como uma *British Standard*, denominado BS 7799, que apresentava as melhores práticas em controles de segurança para auxiliar as organizações comerciais e de governo na implantação e crescimento da segurança da informação. (OLIVA e OLIVEIRA, 2003).

Devido ao interesse internacional em uma norma de segurança da informação, a BS 7799-1:1999 foi submetida a *International Organization for Standardization* (ISO), organização internacional que aglomera os grêmios de padronização/normalização de 148 países. Em dezembro de 2000 a parte 1 BS 7799-1:1999 foi publicada como norma internacional ISO 17799:2000. Em 2001, a Associação Brasileira de Normas Técnicas - ABNT, publicou a versão brasileira da ISO 17799:2000 que ficou com a denominação de NBR/ISO 17799 – Código de Prática para a Gestão da Segurança da Informação. Em setembro de 2005, a norma foi revisada e publicada como NBR ISO/IEC 17799:2005. (ISO 17799, 2005).

A norma ISO/IEC 17799:2005 define 127 controles que compõem o escopo do Sistema de Gestão de Segurança da Informação (*Information Security Management System* – ISMS) agrupados em 11 seções de controles, conforme descrito abaixo:

1. **Política de Segurança da Informação**: recomendações para a formalização de uma política. Contendo: diretrizes, princípios e regras que irão prover orientação e apoio para implantação e manutenção da segurança. Caruso e Steffen (1999) afirmam que a correta implantação de uma política de segurança pode ser resumida em três aspectos: redução da probabilidade de ocorrência, redução dos danos provocados por eventuais ocorrências, e criação de procedimentos para se recuperar de eventuais danos;
2. **Organização da Segurança da Informação**: recomendações para o estabelecimento de uma estrutura de gestão para planejar e controlar a implementação da segurança da informação na organização; (BEAL, 2005, p. 33)
3. **Gestão de Ativos**: recomendações sobre a realização de inventário dos ativos informacionais e atribuição de responsabilidades pela manutenção dos controles necessários para protegê-los;
4. **Segurança em Recursos Humanos**: recomendações para reduzir os riscos de erro humano, roubo, fraude ou uso indevido das instalações;

5. **Segurança Física e do Ambiente**: recomendações para a proteção dos recursos e instalações de processamento de informações críticas ou sensíveis ao negócio contra acesso não autorizado, dano ou interferência;
6. **Gestão das Operações e Comunicações**: recomendações para garantir a operação correta e segura dos recursos de processamento de informações e proteger a integridade de serviços e informações;
7. **Controle de Acesso**: recomendações para a monitoração e o controle do acesso a recursos computacionais, para protegê-los contra abusos internos e ataques externos;
8. **Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação:** recomendações para o uso de controles de segurança em todas as etapas do ciclo de vida forçam que, com todos os esforços de TI, tudo seja implementado e mantido com a segurança em mente, usando controles de segurança em todas as etapas do processo;
9. **Gestão de Incidentes da Segurança da Informação**: recomendações para notificação de fragilidades e eventos de segurança da informação, responsabilidades e procedimentos e coleta de evidências.
10. **Gestão da Continuidade do Negócio:** recomendações para preparar a organização para neutralizar as interrupções às atividades comerciais e proteger os processos críticos em caso de ocorrência de falha ou desastre;
11. **Conformidade:** recomendações para a preservação da conformidade com requisitos legais (tais como direitos autorais e direito à privacidade), com normas e diretrizes internas e com os requisitos técnicos de segurança.

Há uma seção introdutória na norma que trata da Análise, Avaliação e Tratamento de Riscos a fim de orientar na identificação, quantificação e priorização do gerenciamento do risco, bem com os critérios definidos para aceitar o risco ou não (ISO 17799, 2005).

A adequação de qualquer empresa à norma ISO/IEC 17799:2005 garante conformidade com as melhores práticas em gestão da segurança da informação. “As normas são criadas para estabelecer diretrizes e princípios para melhorar a gestão de segurança nas empresas e organizações.” (HOLANDA, 2006).

2.5.2.1 SEÇÕES E CONTROLES DA NORMA 17799:2005

A norma ABNT NBR ISO/IEC 17799 em sua versão 2005, encontra-se estruturada nas seguintes seções e seus respectivos controles:

1. Política de Segurança da Informação
1.1. Política de Segurança da Informação
Objetivo: prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.
1. documento aprovado pela direção, publicado e comunicado para todos os funcionários e terceiros; 2. deve ser analisada criticamente a intervalos planejados ou quando ocorrem mudanças significativas.

2. Organização da Segurança de Informação
2.1. Infra-estrutura da segurança da informação
Objetivo: gerenciar a segurança de informação dentro da organização.
1. a direção deve apoiar ativamente a segurança da informação dentro da organização; 2. as atividades de segurança devem ser coordenadas por representantes de diferentes partes da organização, com funções e papéis relevantes; 3. todas as responsabilidades pela segurança da informação estejam claramente definidas; 4. definir e implementar um processo de gestão de autorização para novos recursos de processamento da informação; 5. definir acordos de confidencialidade e de não divulgação; 6. quando e quais autoridades devem ser contatadas no caso de incidentes de segurança da informação; 7. contatos com grupos de interesse especiais ou outros fóruns especializados e associações profissionais; 8. análise crítica independente da segurança da informação (gerência de outra área ou empresa terceira)
2.2. Partes Externas
Objetivo: manter a segurança dos recursos de processamento da informação e da informação da organização, que são acessados, processados, comunicados ou gerenciados por partes externas.
1. avaliar os riscos de processos de negócios com terceiros implementando controles apropriados antes de se conceder o acesso; 2. considerações sobre o acesso de clientes aos ativos da informação; 3. acordos com terceiros assegurando que não existe mal-entendido entre as partes e possibilidade de indenização.

3. Gestão de Ativos
3.1. Responsabilidade pelos ativos
Objetivo: alcançar e manter a proteção adequada dos ativos da organização.
1. todos os ativos devem ser identificados, inventariados e documentada sua importância; 2. todos os ativos de informação devem possuir um proprietário; 3. definição de regras para uso da informação e dos recursos de processamento da informação (Internet, e-mail, dispositivos móveis);
3.2. Classificação da informação
Objetivo: assegurar que a informação receba um nível adequado de proteção.
1. classificação da informação em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização; 2. definição de um conjunto de procedimentos para rotulação e tratamento da informação, tanto dos ativos da informação no formato físico quanto no eletrônico.

4. Segurança em Recursos Humanos

4.1. Antes da contratação

Objetivo: assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordos com seus papéis e reduzir o risco de roubos, fraudes ou mau uso de recursos.

1. papéis e responsabilidades;
2. seleção;
3. termos e condições de contratação.

4.2 Durante a contratação

Objetivo: assegurar que os funcionários, fornecedores e terceiros estão conscientes das ameaças e preocupações relativas à segurança da informação, de suas responsabilidades e obrigações, e estão preparados para apoiar a política de segurança da informação da organização durante os seus trabalhos normais, e para reduzir o risco de erro humano.

1. responsabilidades da direção;
2. conscientização, educação e treinamento em segurança da informação;
3. processo disciplinar.

4.3 Encerramento ou mudança da contratação

Objetivo: assegurar que os funcionários, fornecedores e terceiros deixem a organização ou mudem de trabalho de forma ordenada.

1. encerramento de atividades;
2. devolução de ativos;
3. retirada de direitos de acesso.

5. Segurança Física e do Ambiente

5.1 Áreas seguras

Objetivo: prevenir o acesso físico não-autorizado, danos e interferências com as instalações e informações da organização.

1. perímetro de segurança física;
2. controles de entrada física;
3. segurança em escritórios, salas e instalações;
4. proteção contra ameaças externas e do meio ambiente;
5. trabalhando em áreas seguras;
6. acesso do público, áreas de entrega e de carregamento.

5.2 Segurança de equipamentos

Objetivo: impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização.

1. instalação e proteção do equipamento;
2. utilidades (falha de energia elétrica);
3. segurança do cabeamento;
4. manutenção dos equipamentos;
5. segurança de equipamentos fora das dependências da organização;
6. reutilização e alienação segura de equipamentos;
7. remoção de propriedade.

6. Gerenciamento das Operações e Comunicações

6.1. Procedimentos e responsabilidades operacionais

Objetivo: garantir a operação segura e correta dos recursos de processamento da informação.

1. documento formal com procedimentos operacionais para: backup, contatos de suporte, recuperação em caso de falha do sistema etc.
2. existência de ambiente separado para recursos de desenvolvimento, teste e produção em sistemas

6.2. Gerenciamento de serviços terceirizados

Objetivo: implementar e manter o nível apropriado de segurança da informação e entrega de serviços em consonância com acordos de entrega de serviços terceirizados.
1. monitoramento dos serviços terceirizados quanto à entrega do serviço, relatórios e possíveis mudanças
6.3. Planejamento e aceitação dos sistemas
Objetivo: minimizar o risco de falhas nos sistemas.
1. implantação de novos sistemas, atualizações e novas versões somente após serem devidamente testados, considerando o impacto na segurança da organização como um todo
6.4. Proteção contra códigos maliciosos e códigos móveis
Objetivo: proteger a integridade do software e da informação.
1. antivírus 2. proibição de uso de softwares não autorizados
6.5. Cópias de segurança
Objetivo: manter a integridade e disponibilidade da informação e dos recursos de processamento da informação.
1. implantação de sistema de backup
6.6. Gerenciamento da segurança em redes
Objetivo: garantir a proteção das informações em redes e a proteção da infra-estrutura de suporte.
1. firewalls 2. sistema de detecção de intrusos - IDS
6.7. Manuseio de mídias
Objetivo: prevenir contra divulgação não autorizada, modificação, remoção ou destruição aos ativos, e interrupções das atividades do negócio.
1. manter as mídias e documentação de sistemas seguras em um ambiente protegido 2. existência de cópia em outro local 3. descarte seguro da mídia removível: incineração ou trituração 4. identificação da classificação da mídia: confidencial, restrita etc
6.8. Troca de informações
Objetivo: manter a segurança na troca de informações e softwares internamente à organização e com quaisquer entidades externas.
1. uso de criptografia na troca de informações, principalmente entre empresas e mensagens com anexos 2. conscientização das pessoas sobre os risco de troca de informações em locais não seguros: corredores, bares, cafés, banheiros, celulares em local público etc. 3. compartilhamento adequado e seguro das informações
6.9. Serviços de comércio eletrônico
Objetivo: garantir a segurança de serviços de comércio eletrônico e sua utilização segura.
1. uso de criptografia de chave pública 2. uso de assinaturas digitais
6.10. Monitoramento
Objetivo: detectar atividades não autorizadas de processamento da informação.
1. monitoramento, proteção e análise crítica dos registros (*logs*) de auditoria com atividades dos usuários, exceções e outros eventos de segurança da informação para assegurar que os usuários estão executando somente as atividades que foram explicitamente autorizadas, melhorar a compreensão das ameaças encontradas no sistema e a maneira pela qual isto pode acontecer 2. sincronização dos relógios de todos os sistemas de acordo com uma hora oficial

7. Controle de Acesso
7.1. Requisitos de negócio para controle de acesso
Objetivo: controlar acesso à informação
1. política de controle de acesso

7.2. Gerenciamento de acesso do usuário
Objetivo: assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação
1. registro de usuário 2. gerenciamento de privilégios 3. gerenciamento de senha do usuário 4. análise crítica dos direitos de acesso de usuário
7.3. Responsabilidade dos usuários
Objetivo: prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou roubo da informação e dos recursos de processamento da informação.
1. uso de senhas 2. equipamento de usuário sem monitoração 3. política de mesa limpa e tela limpa
7.4. Controle de acesso à rede
Objetivo: prevenir acesso não autorizado aos serviços da rede.
1. política de uso dos serviços da rede 2. autenticação para conexão externa do usuário 3. identificação de equipamento em redes 4. proteção e configuração de portas de diagnóstico remotas 5. segregação de redes 6. controle de conexão de rede 7. controle de roteamento de redes
7.5. Controle de acesso ao sistema operacional
Objetivo: prevenir acesso não autorizado aos sistemas operacionais
1. procedimentos seguros de entrada no sistema (*log-on*) 2. identificação e autenticação de usuário 3. sistema de gerenciamento de senha 4. uso de utilitários de sistema 5. desconexão de terminal por inatividade 6. limitação de horário de conexão
7.6. Controle de acesso à aplicação e à informação
Objetivo: prevenir acesso não autorizado à informação contida nos sistemas de aplicação.
1. restrição de acesso à informação 2. isolamento de sistemas sensíveis
7.7. Computação móvel e trabalho remoto
Objetivo: garantir a segurança da informação quando se utilizam a computação móvel e recursos de trabalho remoto.
1. computação e comunicação móvel 2. trabalho remoto

8. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação
8.1. Requisitos de segurança de sistemas de informação
Objetivo: garantir que segurança é parte integrante de sistemas de informação.
1. análise e especificação dos requisitos de segurança
8.2. Processamento correto nas aplicações
Objetivo: prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações.
1. validação dos dados de entrada 2. controle de processamento interno 3. integridade de mensagens 4. validação de dados de saída
8.3. Controles criptográficos
Objetivo: proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos.

1. política para o uso de controles criptográficos 2. gerenciamento de chaves
8.4. Segurança dos arquivos do sistema
Objetivo: garantir a segurança de arquivos de sistema
1. controle de software operacional 2. proteção dos dados para teste de sistema 3. controle de acesso ao código-fonte de programa
8.5. Segurança em processos de desenvolvimento e de suporte
Objetivo: manter a segurança de sistemas aplicativos e da informação.
1. procedimentos para controle de mudanças 2. análise crítica técnica das aplicações após mudanças no sistema operacional 3. restrições sobre mudanças em pacotes de software 4. vazamento de informações 5. desenvolvimento terceirizado de software
8.6. Gestão de vulnerabilidades técnicas
Objetivo: reduzir riscos resultantes da exploração de vulnerabilidades técnicas conhecidas.
1. controle de vulnerabilidades técnicas

9. Gestão de Incidentes de Segurança da Informação
9.1. Notificação de fragilidades e eventos de segurança da informação
Objetivo: assegurar que um enfoque consistente e efetivo seja aplicado a gestão de incidentes da segurança da informação.
1. notificação de eventos de segurança da informação 2. notificando fragilidades de segurança da informação
9.2. Gestão de incidentes de segurança da informação e melhorias
Objetivo: assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes de segurança da informação.
1. responsabilidades e procedimentos 2. aprendendo com os incidentes de segurança da informação 3. coleta de evidências

10. Gestão da Continuidade do Negócio
10.1. Aspectos da gestão da continuidade do negócio, relativos à segurança da informação
Objetivo: não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos e assegurar a sua retomada em tempo hábil se for o caso.
1. incluindo segurança da informação no processo de gestão da continuidade de negócio 2. continuidade de negócios e análise/avaliação de riscos 3. desenvolvimento e implementação de planos de continuidade relativos à segurança da informação 4. estrutura do plano de continuidade do negócio 5. testes, manutenção e reavaliação dos planos de continuidade do negócio

11. Conformidade
11.1. Conformidade com requisitos legais
Objetivo: evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.
1. identificação da legislação vigente 2. direitos de propriedade intelectual 3. proteção de registros organizacionais 4. proteção de dados e privacidade de informações pessoais 5. prevenção de mau uso de recursos de processamento da informação 6. regulamentação de controles de criptografia
11.2. Conformidade com normas e políticas de segurança da informação e conformidade técnica
Objetivo: garantir a conformidade dos sistemas com as políticas e normas organizacionais de segurança da informação.
1. conformidade com as políticas e normas de segurança da informação 2. verificação da conformidade técnica
11.3. Considerações quanto à auditoria de sistemas de informação
Objetivo: maximizar a eficácia e minimizar a interferência no processo de auditoria dos sistemas de informação.
1. controles de auditoria de sistemas de informação 2. proteção de ferramentas de auditoria de sistemas de informação

2.5.3 ISO/IEC 27001

A ISO/IEC 27001 é a norma que trata de Sistemas de Gestão de Segurança da Informação. Sua utilização está diretamente relacionada à ISO/IEC 17799:2005.

> A nova família da série ISO IEC 27000-27009 está relacionada com os requisitos mandatários da ISO/IEC 27001:2005, como, por exemplo, a definição do escopo do Sistema de Gestão da Segurança da Informação, a avaliação de riscos, a identificação de ativos e a eficácia dos controles implementados. (HOLANDA, 2006).

Hoje, se uma empresa brasileira desejar obter a certificação em Gestão da Segurança da Informação, deve se adequar às práticas determinadas na NBR/ISO 17799:2005 e ser auditada conforme os padrões estabelecidos na NBR/ISO 27001:2006, uma revisão atualizada da BS 7799-2. De acordo com a empresa de segurança Módulo (2005), existem no mundo 194 empresas certificadas pela BS 7799-2, das quais 192 em países como Reino Unido (82), Japão (21), Coréia (9), Índia (9), Alemanha (8), Finlândia (8). No Brasil existem duas empresas certificadas: o SERASA-SP e a própria Módulo Security, sendo que a empresa Módulo Security encontra-se certificada pela NBR/ISO 27001:2006.

Fundamentando a escolha do tema gestão da segurança da informação em pequenas e médias empresas, Holanda (2006) corrobora afirmando que a maioria das organizações, independentemente do seu porte ou ramo de atuação, podem fazer uso da norma ISO/IEC 27001:2006.

Ainda segundo Holanda (2006), o comitê que trata da segurança da informação na ISO aprovou a criação de uma família de normas sobre gestão da segurança da informação, batizada pela série 27000.

Título	Objetivo	Situação Atual
ISO IEC NWIP 27000 *Information Security Management Systems - Fundamentals and Vocabulary*	Apresentar os principais conceitos e modelos relacionados com segurança da informação.	Encontra-se ainda nos primeiros estágios de desenvolvimento, denominado de *NWIP-New Work Item Proposal*. A previsão para publicação como norma internacional é 2008-2009.
ISO IEC 27001:2005 *Information Security Management Systems – Requirements*.	Esta norma é aplicável a qualquer organização, independente do seu ramo de atuação, e define requisitos para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar um Sistema de Gestão de Segurança da Informação. A ISO IEC 27001 é a norma usada para fins de certificação e substitui a norma Britânica BS 7799-2:2002. Portanto, uma organização que deseje implantar um SGSI deve adotar como base a ISO IEC 27001.	Norma aprovada e publicada pela ISO em Genebra, em 15/10/2005 e no Brasil pela ABNT em 2006.
ISO IEC 27002:2005 *Information Technology - Code of practice for information Security Management*.	É um guia prático que estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos de controle e os controles definidos nesta norma têm como finalidade atender aos requisitos identificados na análise/avaliação de riscos.	Norma aprovada e publicada pela ISO em Genebra, em 15/06/2005. No Brasil, a ABNT publicou como Norma Brasileira NBR ISO IEC 17799 no dia 24 de agosto de 2005.
ISO IEC 1 st WD 27003 *Information Security Management Systems-Implementation Guidance*.	Fornecer um guia prático para implementação de um Sistema de Gestão da Segurança da Informação, baseado na ISO IEC 27001.	Encontra-se em um estágio de desenvolvimento, denominado de *WD-Working Draft*. A previsão para publicação como norma internacional é 2008-2009.
ISO IEC 2nd WD 27004 *Information Security Management-Measurements*	Fornecer diretrizes com relação a técnicas e procedimentos de medição para avaliar a eficácia dos controles de segurança da informação implementados, dos processos de segurança da informação e do Sistema de Gestão da Segurança da Informação.	Encontra-se em um estágio em que vários comentários já foram discutidos e incorporados ao projeto. A previsão para publicação como norma internacional é 2008-2009.
ISO IEC 2nd CD 27005 *Information Security Management Systems-Information Security Risk Management.*	Fornece diretrizes para o gerenciamento de riscos de segurança da informação.	Encontra-se em um estágio mais avançado, pois vem sendo discutido há mais de dois anos. A previsão para publicação como norma internacional é em 2007.

Quadro 1: normas ISO série 27000

2.6 DOMÍNIOS DA SEGURANÇA DA INFORMAÇÃO

Para facilitar o estudo e o entendimento dos diversos controles da norma ISO 17799, os autores Adachi e Diniz (2005), Sêmola (2003) e Beal (2005) propuseram sua divisão em dez domínios. Os autores Adachi e Diniz ainda os classificou nas três camadas de segurança da informação. Os próximos quadros exibem essa divisão, comparando-as com as seções apresentadas da norma ISO/IEC 17799:2005.

Adachi e Diniz		**ISO/IEC 17799:2005**	
Domínio	**Camada**	**Seções**	**Camada**
Arquitetura e modelos de segurança	física	Política de segurança da informação Gestão de Ativos	humana
Sistemas de controle de acesso	física	Controle de acesso	física
Segurança em telecomunicação e redes	física	Gestão das operações e comunicações	física
Segurança física	física	Segurança física e do ambiente	física
Desenvolvimento de sistemas e aplicativos	lógica	Aquisição, desenvolvimento e manutenção de sistemas de informação	lógica
Criptografia	lógica	-	-
Práticas de gerenciamento de segurança	humana	Organizando a segurança da informação	humana
Segurança de Operação	humana	-	-
Legislação, investigação e ética	humana	Conformidade	humana
Plano de continuidade do negócio e plano de recuperação em caso de desastre	humana	Gestão da continuidade do negócio	humana
		Segurança em recursos humanos	humana
		Gestão de incidentes de segurança da informação	física

Quadro 2: comparação entre o modelo de Adachi e Diniz e a norma ISO 17799

Sêmola e Beal	**ISO/IEC 17799:2005**	
Domínio	**Seções**	**Camada**
Política de segurança	Política de segurança da informação	humana
Segurança organizacional	Organizando a segurança da informação	humana
Classificação e controle dos ativos da Informação	Gestão de Ativos	humana
Segurança em pessoas	Segurança em recursos humanos	humana
Segurança física e do ambiente	Segurança física e do ambiente	física
Gestão das operações e comunicações	Gestão das operações e comunicações	física
Controle de Acesso	Controle de acesso	física
Manutenção e desenvolvimento de sistemas	Aquisição, desenvolvimento e manutenção de Sistemas de Informação	lógica
Gestão da continuidade do negócio	Gestão da continuidade do negócio	humana
Conformidade	Conformidade	humana
	Gestão de incidentes de segurança da informação	física

Quadro 3: comparação entre os domínios de Sêmola e Beal e a norma ISO 17799

Neste trabalho foram utilizadas as seções da norma ISO 17799 divididas nas três camadas conforme abaixo:

Camada	Seção	Objetivos
Física	Gestão das operações e comunicações	garantir a operação segura e correta dos recursos de processamento da informação.
	Segurança física e do ambiente	prevenir o acesso físico não-autorizado, danos e interferências com as instalações e informações da organização; impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização.
	Controle de acesso	controlar acesso à informação; assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação; prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou roubo da informação e dos recursos de processamento da informação; prevenir acesso não autorizado aos serviços da rede.
	Gestão de incidentes de segurança da informação	assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes da segurança da informação.
Lógica	Aquisição, desenvolvimento e manutenção de Sistemas de Informação	garantir que segurança é parte integrante de sistemas de informação; prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações; proteger a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos; garantir a segurança de arquivos de sistema; manter a segurança de sistemas aplicativos e da informação. reduzir riscos resultantes da exploração de vulnerabilidades técnicas conhecidas.
Humana	Organizando a segurança da informação	gerenciar a segurança de informação dentro da organização; manter a segurança dos recursos de processamento da informação e da informação da organização, que são acessados, processados, comunicados ou gerenciados por partes externas.
	Gestão de Ativos	alcançar e manter a proteção adequada dos ativos da organização; assegurar que a informação receba um nível adequado de proteção.
	Segurança em recursos humanos	assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com seus papéis e reduzir o risco de roubos, fraudes ou mau uso de recursos.
	Gestão da continuidade do negócio	não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos e assegurar a sua retomada em tempo hábil se for o caso.
	Conformidade	evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.
	Política de segurança da informação	prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

Quadro 4: seções da norma ISO 17799 por camadas

Muitas seções da norma ISO/IEC 17799:2005 possuem características das três camadas de segurança da informação (física, lógica e humana). Houve um esforço neste trabalho no sentido de classificar a seção pela camada que apresenta a maioria dos controles de uma delas.

Apesar da norma ISO/IEC 17799:2005 tratar em seu escopo de 127 controles, nem todos podem ser implementados devido à complexidade e custo de implantação, para tanto, conforme recomendação da própria norma "a relevância de qualquer controle deve ser determinada segundo os riscos específicos a que uma organização está exposta." (ISO 17799, 2005).

Segundo recomendações da norma os controles considerados essenciais para uma organização são:

a) proteção de dados e privacidade de informações pessoais;

b) proteção de registros organizacionais;

c) direitos de propriedade intelectual.

Outros controles considerados práticas para a segurança da informação incluem:

a) documento da política de segurança da informação;

b) atribuição de responsabilidades para a segurança da informação;

c) conscientização, educação e treinamento em segurança da informação;

d) processamento correto nas aplicações;

e) gestão de vulnerabilidades técnicas;

f) gestão da continuidade do negócio;

g) gestão de incidentes de segurança da informação e melhorias.

2.7 CONCEPÇÕES ERRÔNEAS ACERCA DA SEGURANÇA

Segundo Caruso e Steffen (1999), existem algumas concepções errôneas sobre segurança que foram criadas com o tempo dentro das empresas e que merecem esclarecimento:

- **Uma vez implantada a segurança, as informações estão seguras:** a segurança nunca será um produto acabado, pois reflete o atual ambiente de informações das organizações modernas, altamente dinâmico.
- **A implantação da segurança é um processo simples:** a implantação da segurança deve ser um processo gradual; o maior esforço recai sobre os usuários dos sistemas de informação, pois é neles que reside o conhecimento do que é importante para ser protegido.
- **A segurança é um assunto de exclusiva responsabilidade da área de segurança:** é o proprietário das informações que deve avaliar o que deve ou não ser protegido; dessa forma, a segurança também passa a ser assunto de sua responsabilidade.
- **A estrutura de segurança é relativamente estática:** da mesma maneira que outras estruturas na empresa sofrem mudanças, a estrutura de segurança deve ser dinâmica o suficiente para acompanhar tais mudanças.

Sêmola (2003) contribui com a visão de Caruso e Steffen (1999) afirmando que muitos erros são praticados na gestão da segurança da informação pela visão míope e a percepção distorcida do problema, pois muitos gestores enxergam somente os problemas associados à tecnologia como: Internet, redes, computadores, e-mail, vírus e *hacker*. Em função desse entendimento parcial, o autor lista uma série de concepções errôneas acerca da gestão da segurança da informação:

- Atribuir exclusivamente à área tecnológica a segurança da informação;
- Posicionar hierarquicamente essa equipe abaixo da diretoria de TI;
- Definir investimentos subestimados e limitados à abrangência dessa diretoria;
- Elaborar planos de ação orientados à reatividade;

- Não perceber a interferência direta da segurança com o negócio;
- Tratar as atividades como despesa e não como investimento;
- Adotar ferramentas pontuais como medida paliativa;
- Satisfazer-se com a sensação de segurança provocada por ações isoladas;
- Não cultivar corporativamente a mentalidade de segurança;
- Tratar a segurança como um projeto e não como um processo.

2.8 TECNOLOGIA DA INFORMAÇÃO EM PEQUENAS E MÉDIAS EMPRESAS

Devido ao fato da maioria das informações de negócio das organizações modernas estarem armazenadas em microcomputadores e haver vasta utilização dos recursos de TI para sustentar o negócio, vê-se como importante e fundamental estudar as empresas que adotam esses recursos e sua dependência a eles, de forma que, quanto mais dependente de um recurso de TI, maior deve ser sua preocupação com a gestão da segurança da informação. Em particular, as pequenas e médias empresas, por possuírem menores recursos financeiros e humanos comparados as grandes organizações, um processo de tomada de decisão geralmente centralizado em uma ou duas pessoas e a falta ou quase inexistência de burocracia.

A TI tem transformado muitas organizações nas últimas décadas, mas somente após o advento do microcomputador na década de 80, é que o impacto começou a atingir as pequenas e médias empresas no mundo. Com a abertura comercial da Internet, as possibilidades de uso da TI por pequenas e médias empresas se multiplicarão, pois custos de equipamentos, serviços e produtos entraram em queda constante, além do aumento da oferta de soluções.

“Não há mais dúvidas de que para as funções da administração – planejamento, organização, liderança e controle – são de suma importância os sistemas que fornecem informações aos administradores” (Prates e Ospina, 2004, p. 10). A qualidade e precisão dessas informações são decisivas para transformar os objetivos traçados em planos concretos, seja em qualquer tipo ou tamanho de organização.

A pequena e a média empresa que durante o período inicial de desenvolvimento da TI foram classificadas por fornecedores como público-alvo secundário, ganham espaço nas discussões de planejamento de mercado dessas empresas, sejam grandes ou pequenos fornecedores. Devido principalmente à estagnação do mercado das grandes empresas, que em sua grande maioria, possuem as mais diversas ferramentas de TI e recursos humanos qualificados para operá-los.

Independente do tamanho da empresa, a TI pode auxiliar nos processos operacionais, bem como na tomada de decisão: coletando, analisando e fornecendo informações para o andamento do negócio. Porém na pequena e média empresa, os recursos disponíveis são mais escassos que na grande empresa, o que as limita a investirem em tecnologias maduras e amplamente divulgadas no mercado, de maneira a aliviar os riscos.

“Nos países de primeiro mundo, a TI tem sido considerada como um dos fatores responsáveis pelo sucesso das organizações, tanto no âmbito de sobrevivência, quanto no aumento da competitividade.” (YOUG apud Prates e Ospina, 2004). Para Lunardi e Dolci (2006) citando Leite “em muitos casos a TI é vista como um ‘mal necessário’: concorda-se em tê-la, mas busca-se minimizar cada vez mais o transtorno de aumentar o seu total de recursos investidos”.

Prates e Ospina (2004) argumentam que os administradores investem em novas ferramentas de TI, porque acreditam no aumento da velocidade de suas operações e na diminuição do custo associado, e o fazem para atingir objetivos estratégicos e para planejar e alcançar um ou mais dos três objetivos operacionais independentes:

- Aumentar a continuidade - integração funcional, automação intensificada, resposta rápida;
- Melhorar o controle – precisão, acuidade, previsibilidade, consistência, certeza;
- Proporcionar maior compreensão das funções produtivas – visibilidade, análise, síntese.

No Brasil, segundo Prates e Ospina (2004), as pequenas empresas possuem informatização apenas em processos operacionais isolados e não se extraem informações relevantes para a tomada de decisão, nem do ambiente interno e muito menos do ambiente externo da empresa. Assim, um sistema de informação voltado para a pequena empresa (e média) deve respeitar alguns quesitos: custo, tempo e qualidade.

2.9 FATORES INFLUENCIADORES PARA ADOÇÃO DE TI EM PEQUENAS E MÉDIAS EMPRESAS

Pouca literatura foi encontrada sobre a adoção da gestão da segurança da informação em organizações de qualquer porte. Porém, devido ao fato de a maioria das pessoas entender segurança da informação como simplesmente segurança de rede ou segurança em TI, e a confusão gerada a partir disso, buscou-se entender os motivos para a adoção de TI como forma de entendimento para a adoção da gestão da segurança da informação. Seguem os autores pesquisados e suas considerações:

Thong (apud Prates e Ospina, 2004) salienta que as pequenas empresas não conhecem a importância de fatores-chave em TI, além de disporem de recursos reduzidos, e podem estar gastando recursos e energia em fatores de pouca importância para o sucesso da implementação da TI. O autor, em pesquisa realizada com 114 pequenas empresas de Singapura, concluiu que as pequenas empresas com sucesso em TI tendiam a ter alta participação de especialistas externos, investimento adequado, alto conhecimento dos usuários, alto grau de envolvimento do usuário e alto suporte do gerente geral. Porém a chave principal do sucesso de implantação da TI seria a alta participação do especialista externo.

Palvia e Palvia (1999) conduziram uma pesquisa em uma amostra de 1460 pequenas empresas para verificar os padrões de satisfação com TI - onde o proprietário era também gerente, principal usuário, além de desempenhar as principais atividades de TI. Os autores concluíram que as características do proprietário têm impacto maior na satisfação em TI do que qualquer outro fator; para tanto foram considerados gênero, idade do proprietário, raça e habilidade em computação.

Outra pesquisa foi conduzida por Anandajaran, Igbaria e Anakwe (apud Prates e Ospina, 2004) com dados coletados de 143 usuários na Nigéria, a fim de determinar os fatores que motivam os usuários a aceitar a TI. Os resultados apontaram que a pressão social é um importante fator.

Em pesquisa realizada com 25 pequenas empresas da macro-região de Ribeirão Preto – SP, Prates e Ospina (2004), identificaram que os principais motivos que levaram as empresas a implantar TI foram:

- melhoria dos controles organizacionais;
- aumento de participação no mercado;
- aumento de produtividade;
- redução de custos.

Em relação às dificuldades encontradas, a resistência pelos funcionários foi a mais expressiva com média 3,2 (numa escala de pontos de 1 a 5), seguida pela cultura tradicional e ausência de pessoal qualificado. O fator: falhas de segurança recebeu média 1,6 ficando em 13º de um total de 16 fatores pesquisados. Como a maioria das empresas pesquisadas (72,2%) estão no estágio 1 (iniciação) ou 2 (contágio) da escala de Nolan apresentada no quadro 5. Conclui-se que essas possuem pouca ou nenhuma dependência da TI em seus processos de negócios, assim a perda, fraude ou furto de tais sistemas ou informações pode não ser considerados importantes.

Os autores ainda pesquisaram os fatores de êxito para utilização de TI chegando aos seguintes resultados, em ordem de importância:

- percepção da necessidade pelos usuários;
- apoio da cúpula executiva;
- treinamento adequado;
- aceitação por toda a organização;
- dedicação da equipe de implementação;
- responsabilidade do gerente de operações e

- superação de barreiras sócio-culturais.

Cragg e King (1993) pesquisaram os fatores motivadores e inibidores para utilização de computadores em pequenas empresas. Como fatores motivadores encontraram o que nomearam como *relative advantage* que se refere:

- às economias de tempo e esforço;
- benefícios econômicos e
- diminuição de muitas tarefas repetidas.

Estágio I	Iniciação	Neste estágio os usuários estão assustados e surpreendidos com a tecnologia, não existe planejamento nem controle de tecnologia ou processamento de dados suficientes.
Estágio II	Contágio	Durante este estágio existe um encorajamento por parte da organização para aplicação extensiva de tecnologia, porém problemas são criados pela inexperiência dos programadores, que trabalham sem os benefícios de um efetivo sistema de controle gerencial.
Estágio III	Controle	É caracterizada pela reestruturação e profissionalização da atividade de processamento de dados, melhorando sua reputação na organização.
Estágio IV	Integração	Este estágio é atingido quando as mudanças iniciadas no estagio anterior são realizadas por completo e os usuários que já tinham desistido começam a ganhar algo novo, como tecnologia de banco de dados e terminais interativos.
Estágio V	Administração de Dados	Os usuários começam a ter uma postura mais participativa. O enfoque deste estágio está no compartilhamento de bases de dados únicas pelos sistemas de informações.
Estágio VI	Maturidade	A carteira de aplicações é completada e sua estrutura espelha a organização e seus fluxos de informações.

Quadro 5: estágios de crescimento de TI, segundo Nolan
Fonte: Albertin (2004).

O entusiasmo de alguns proprietários com a tecnologia e a forte influência de consultores de TI também foram fatores considerados como motivadores da adoção. Os fatores que desencorajaram o crescimento de TI foram agrupados em: educacionais, tempo administrativo, econômicos e técnicos. Os fatores educacionais são relativos à falta de conhecimento sobre os sistemas utilizados, bem como falta de pessoas com conhecimentos específicos de análise de sistemas, *design* e desenvolvimento. Referente ao fator tempo administrativo, muitos sistemas que são freqüentemente adquiridos para economizar tempo, bem como reduzir custos, acabam consumindo considerável quantia de tempo dos gerentes no processo de implantação. Os fatores econômicos referem-se à situação econômica da empresa no momento e à análise informal de custo-benefício dos sistemas. Com pouco

conhecimento técnico interno, pequenas empresas são muito confiantes no conselho e apoio que obtêm de seus fornecedores de TI, o que as limita muitas vezes ao uso de pacotes de aplicativos, à aceitação de limitações no software e a sua adaptação aos requerimentos do sistema.

Lunardi e Dolci (2006) realizaram uma pesquisa com 123 micros e pequenas empresas (MPEs) do Rio Grande do Sul a fim de analisar o relacionamento existente entre a adoção de TI e o seu impacto no desempenho organizacional percebido destas empresas. Os principais motivos que têm levado as MPEs a adotarem TI estão relacionadas às:

- pressões externas (os concorrentes diretos têm adotado ou por influência de clientes, fornecedores ou do próprio governo) que a empresa enfrenta e
- à existência de um ambiente organizacional favorável (funcionários em condições de utilizá-la e com uma estrutura organizacional adequada).

Relacionado à gestão da segurança da informação, Gupta e Hammond (2004), realizaram uma pesquisa com 138 pequenas e médias empresas nos Estados Unidos que apontou como maior preocupação, considerando as várias fontes de ameaças à segurança, os vírus, seguido por: falha de energia, problemas em softwares, integridade dos dados, integridade das transações e segredo dos dados. Somente 19% dos pesquisados alegaram um incidente de segurança nos últimos 12 meses, isto pode explicar a baixa porcentagem de pequenas empresas que desenvolve uma política de segurança e adquire proteção básica e *software* de *backup*.

Gabbay (2003), em sua dissertação de mestrado, estudou os fatores que influenciam os Executivos e Gerentes de TI das empresas com maior contribuição de ICMS no Rio Grande do Norte nas suas percepções em relação às diretrizes de Segurança da Informação na norma NBR ISO/IEC 17799 – dimensão controle de acesso. Em sua conclusão evidenciou a associação entre as variáveis tamanho do parque de informática e a freqüência dos ataques sofridos com a variável “Nível de concordância em relação à norma NBR ISO/IEC 17799 – dimensão controle de acesso”.

3 METODOLOGIA

3.1 TIPO DE PESQUISA

Essa pesquisa utilizou o método exploratório-descritivo. De acordo com Gil (2002, p. 42) “as pesquisas descritivas têm como objetivo primordial a descrição das características de determinada população ou fenômeno ou, então, o estabelecimento de relações entre variáveis”. Ainda segundo o autor, as pesquisas descritivas têm por objetivo levantar as opiniões, atitudes e crenças de uma população. Para tanto, foi realizada pesquisa bibliográfica de forma a aprofundar os conceitos sobre o tema e posteriormente o levantamento dos dados em campo, através da coleta de resposta aos questionários enviados às empresas selecionadas numa base de dados, fornecida pelo Centro das Indústrias do Estado de São Paulo (CIESP).

Gil (2002) considera que o levantamento é o procedimento técnico mais adequado a ser utilizado em pesquisas descritivas, visto que “procede-se à solicitação de informações a um grupo significativo de pessoas acerca do problema estudado para, em seguida, mediante análise quantitativa, obterem-se as conclusões correspondentes aos dados coletados”. Para Appolinário (2006), o levantamento “tem por finalidade investigar as características de determinada realidade ou mesmo descobrir as variáveis componentes dessa realidade”. Gil (2002) acrescenta que os levantamentos trazem as seguintes vantagens: conhecimento direto da realidade (evita subjetivismo dos pesquisadores), economia e rapidez (dados obtidos por questionários têm custos relativamente baixos), quantificação (possibilidade de análise estatística, com o uso de correlações e outros procedimentos).

3.2 AMOSTRA E SUJEITOS DA PESQUISA

A população foi constituída por 1348 indústrias situadas na região do Grande ABC listadas em cadastro do CIESP. Devido à dificuldade de contato com todas as empresas, foi selecionada uma amostra não probabilística por conveniência, do setor mais expressivo do cadastro.

O código CNAE que concentrou o maior número de empresas foi o código 28 – fabricação de produtos de metal, exclusive máquinas e equipamentos – com 256 empresas cadastradas, sendo 225 classificadas como empresas de pequeno porte e 31 empresas classificadas como médio porte pelo próprio cadastro.

Os sujeitos da pesquisa foram os gestores (gerentes ou proprietários) ou analistas que possuem algum envolvimento no processo de aquisição ou em investimentos em gestão da segurança da informação ou em TI.

Tabela 1: distribuição por atividade de pequenas e médias empresas

CNAE	Registros	% Total	Descrição do CNAE
15	54	4,0%	FABRICAÇAO DE PRODUTOS ALIMENTICIOS E BEBIDAS
17	27	2,0%	FABRICAÇAO DE PRODUTOS TEXTEIS
18	24	1,8%	CONFECÇAO DE ARTIGOS DO VESTUARIO E ACESSORIOS
19	4	0,3%	PREPARAÇAO DE COUROS E FABRICAÇAO DE ARTEFATOS DE COURO, ARTIGOS DE VIAGEM E CALÇADOS
20	15	1,1%	FABRICAÇAO DE PRODUTOS DE MADEIRA
21	31	2,3%	FABRICAÇAO DE CELULOSE, PAPEL E PRODUTOS DE PAPEL
22	49	3,6%	EDIÇAO, IMPRESSAO E REPRODUÇAO DE GRAVAÇOES
23	1	0,1%	REFINO DE PETRÓLEO
24	140	10,4%	FABRICAÇAO DE PRODUTOS QUIMICOS
25	204	15,1%	FABRICAÇAO DE ARTIGOS DE BORRACHA E DE MATERIAL PLASTICO
27	58	4,3%	METALURGIA BASICA
28	256	19,0%	FABRICAÇAO DE PRODUTOS DE METAL - EXCLUSIVE MAQUINAS E EQUIPAMENTOS
29	178	13,2%	FABRICAÇAO DE MAQUINAS E EQUIPAMENTOS
31	53	3,9%	FABRICAÇAO DE MAQUINAS, APARELHOS E MATERIAIS ELÉTRICOS
32	15	1,1%	FABRICAÇAO DE MATERIAL ELETRONICO E DE APARELHOS E EQUIPAMENTOS DE COMUNICAÇOES
33	24	1,8%	FABRICAÇAO DE EQUIPAMENTOS DE INSTRUMENTAÇAO MÉDICO-HOSPITALARES, INSTRUMENTOS DE PRECISAO E OPTICOS, EQUIPAMENTOS PARA AUTOMAÇAO INDUSTRIAL, CRONOMETROS E RELOGIOS
34	79	5,9%	FABRICAÇAO E MONTAGEM DE VEICULOS AUTOMOTORES, REBOQUES E CARROCERIAS
35	4	0,3%	FABRICAÇAO DE OUTROS EQUIPAMENTOS DE TRANSPORTE
36	103	7,6%	FABRICAÇAO DE MOVEIS E INDUSTRIAS DIVERSAS
37	3	0,2%	RECICLAGEM
45	26	1,9%	CONSTRUÇAO
	1348	**100,0%**	

3.3 INSTRUMENTO DA PESQUISA

Foram realizadas entrevistas semi-estruturadas com gestores de modo a levantar os principais motivos que os levam a investir em gestão da segurança da informação, quais são os principais riscos percebidos e seu nível de conhecimento sobre o assunto. As questões foram agrupadas em: perfil do gestor, perfil da empresa, valor das informações, análise de risco, ferramentas e técnicas de defesa e fatores (motivadores e inibidores). Após a entrevista, foi confeccionado um questionário eletrônico utilizando informações da literatura da área e algumas das respostas mais expressivas da entrevista.

3.3.1 ENTREVISTAS PARA CRIAÇÃO DO QUESTIONÁRIO

Para fornecer subsídios para criação do questionário, foram realizadas entrevistas semi-estruturadas com sete gestores de quatro organizações diferentes. As entrevistas foram realizadas no mês de setembro de 2006, foram gravadas e tiveram duração aproximada de quarenta minutos. Em três empresas, as entrevistas foram realizadas com dois gestores simultaneamente, somente em uma das empresas, a entrevista foi individual. Por serem semi-estruturadas, as entrevistas permitiram o acompanhamento da resposta e quando necessário, foram efetuadas perguntas relacionadas, que não estavam incluídas no roteiro original. Isso ajudou, segundo defendido por Hair, Jr. et al. (2005), na descoberta de informações adicionais.

A entrevista em profundidade, segundo Hair, Jr. et al. (2005), consiste em uma discussão individual entre o entrevistador e o entrevistado, e permite uma sondagem muito mais profunda dos temas a serem discutidos. Ainda segundo o autor, as entrevistas pessoais são tradicionalmente usadas para obter informações qualitativas detalhadas, a partir de um número relativamente pequeno de indivíduos.

Procurou-se nas entrevistas conhecer primeiramente o perfil do gestor entrevistado, questionando-o sobre incidentes pessoais de segurança ocorridos anteriormente e como ele se mantém informado sobre assuntos ligados a TI e à segurança da informação. Buscou-se levantar também o perfil da empresa e saber o conhecimento do gestor sobre incidentes ocorridos com sua empresa. O valor da informação e o risco inerente a ela também foi objeto de questionamento, de forma a entender como as empresas têm lidado com esse tema. Por fim a entrevista questionou-os sobre as ferramentas e técnicas de defesa implantadas na empresa e os motivos que contribuíram ou contribuiriam para elevar os investimentos em gestão da segurança da informação.

3.3.2 PRINCIPAIS RESULTADOS DAS ENTREVISTAS

Perfil do Gestor

Dos sete gestores entrevistados, somente dois alegaram incidentes pessoais relacionados à segurança da informação, causados principalmente por vírus. Durante a entrevista, pôde-se perceber a desconfiança de dois gestores em realizar suas transações pela Internet ou outro meio digital, preferindo o método tradicional.

Todos os pesquisados disseram não se manter informados sobre notícias ou informações específicas relacionadas a TI ou à gestão da segurança da informação. Quando recebem alguma informação geralmente é por amigos, especialistas da área ou em mídias de divulgação geral como jornais e telejornais.

Perfil da Empresa

Os entrevistados pertencem a organizações de ramos distintos, sendo:

- empresa 1 – ramo de atividade: confecção de brindes, aproximadamente 60 funcionários e 15 computadores em uso;
- empresa 2 – ramo de atividade: refrigeração industrial, aproximadamente 160 funcionários e 102 computadores em uso;
- empresa 3 – ramo de atividade: liga de alumínio, aproximadamente 80 funcionários e 40 computadores em uso;
- empresa 4 – ramo de atividade: mão-de-obra temporária e efetiva, aproximadamente 20 funcionários administrativos-diretos e 25 computadores em uso.

Quando perguntados sobre incidentes de segurança da informação ocorridos na empresa, somente um dos gestores não soube responder; todos os demais já passaram por incidentes como furto de agendas com informações do negócio, perda de informações causadas por vírus, indisponibilidade da informação por paradas não esperadas na rede ou servidores. A maioria das medidas tomadas foi reativa, ou seja, só ocorreram após o incidente.

Valor da Informação

Na empresa 1 não existe maior preocupação com o valor das informações, isso pode ser explicado pelo perfil do gestor entrevistado, por sua pouca idade e por ser filho do proprietário. Porém responde pela área de TI e pelos investimentos em segurança da informação.

Na empresa 2 onde a entrevista foi conduzida com o diretor financeiro, esse mostrou um maior zelo com a informação e sua preocupação com o *lay-out* da empresa, que segundo o mesmo, representa uma ameaça à segurança das informações por não possuir divisórias entre os departamentos, dizendo: “ganha-se em comunicação, mais perde-se em segurança”. A empresa não possui qualquer tipo de classificação das informações implantada, a mesma é dada pela percepção da gerência. Esse gestor em especial demonstrou uma grande preocupação com o valor das informações ao afirmar que sem ela a empresa efetivamente pára: “hoje existe uma necessidade da informação extrema, o ponto zero da empresa, ou seja, sem a informação não fazemos nada. A empresa tem uma real necessidade dos recursos de informação e de TI.”

Os demais gestores mostraram sua preocupação principalmente com informações armazenadas em recursos de TI, quem sabe pelo fato de não conhecerem efetivamente o modo de controlá-las.

Análise de Risco

Sobre o risco de perda de informações, os pesquisados evidenciaram várias preocupações como segue:

- empresa 1 - acredita que existe um risco de perda de informações, mas que essa informação é fácil de ser recuperada pelos vários documentos que compõem a venda ou orçamento, como notas fiscais e pagamento de comissão (feita por funcionário ligado à família – confiança). Explicitou o medo de acesso externo efetuado por *hackers*.
- empresa 2 – citou o uso do *backup* diário como forma de minimizar o risco, mas declarou seu medo com o pessoal interno, que com conhecimentos

necessários, poderiam manusear a base de dados da empresa e copiar informações; disse não saber como controlar isso, e o que resta é a confiança em funcionários e terceiros.

- empresa 3 – considera a maior ameaça à segurança das informações os próprios funcionários, pois possuem acesso aos dados e às informações da empresa. “Com os funcionários, corremos o risco; não tem como fazer de forma diferente.”
- empresa 4 – considera grande o risco de um incidente de segurança da informação e principalmente o impacto desse risco. Um incidente num recurso de TI é mais problemático do que em papel.

Ferramentas e Técnicas de Defesas

Todas as empresas utilizam cópia de segurança (*backup*) e software antivírus como medida de segurança, porém alguns gestores mostraram maior preocupação com o *backup* diário e a recuperação desta informação. Somente na empresa 2 foram citados o uso do *firewall* e campanhas de conscientização dos funcionários para segurança da informação.

Perguntados sobre o possível compartilhamento de senhas de acesso à rede pelos funcionários, todos disseram acreditar que não acontece em suas empresas.

O gestor da empresa 2 disse que foi alertado por sua assessoria que na área de gestão da informação o mais importante do que se ter um bom prestador serviço é ter um bom contrato de serviço.

O gestor da empresa 3 possui processos internos para evitar a engenharia social, como não fornecer informação por telefone, somente por escrito. Existe uma política de informática sobre o que se pode ou não fazer com os recursos de TI.

Na empresa 4, não possuem nenhum tipo de controle sobre o uso dos recursos de TI, acreditam ser coisa de grandes empresas e levantaram a questão de que ao alertar pode-se também motivar o funcionário a fazer a ação.

Fatores (motivadores ou inibidores)

Em todas as empresas, a orientação de um especialista externo ou fornecedor de TI foi motivadora para implantação de algum recurso para a gestão da segurança da informação. A empresa 2 citou também as recomendações de sua auditoria.

O gestor da empresa 3 só investiria mais em segurança caso perdesse algo que não esperava e acha importante verificar a relação custo/benefício do investimento, porém sem ser paranóico. Avaliar a relevância do risco, pois se fosse depender do pessoal de TI estaria totalmente enclausurado. Alegou existir a dificuldade de enxergar o benefício desse investimento.

Na empresa 4, o fato de ocorrer um incidente no departamento financeiro contribuiu para mudança dos processos internos, de forma a aumentar a segurança.

Perfil do Gestor	Não se mantêm informados sobre a área (falta de conhecimento).
Perfil da Empresa	Enfrentaram incidentes de segurança relacionados a: vírus, parada da rede ou servidor, furto de informações.
Valor da Informação e Análise de Risco	A maioria dos gestores alegaram preocupação com as informações armazenadas em TI; Alguns gestores alegaram que o principal risco são os funcionários.
Ferramentas e Técnicas de Defesas	Antivírus; Backup; *Firewall*.
Fatores	Orientação de um especialista externo; Importância da relação custo/benefício do investimento; Incidentes anteriores.

Quadro 6: principais contribuições das entrevistas

3.3.3 QUESTIONÁRIO

O questionário foi disponibilizado às empresas pesquisadas em um *web site* da Internet dividido em quatro etapas. A primeira refere-se à apresentação da pesquisa e ao modo de contato com o pesquisador, de forma a imprimir maior confiança para os pesquisados. Na segunda etapa, foram efetuadas perguntas referentes ao perfil do gestor, perfil da empresa, nível de utilização de TI e das ferramentas e técnicas em segurança da informação. A terceira etapa questionou sobre os fatores que, na percepção do gestor, contribuem para a adoção da gestão da segurança da informação ou a inibem. À quarta e última etapa coube um agradecimento pelas respostas.

Grupo de Variáveis	O que se pretende investigar	Qtde Questões	Exemplos de Questões
Perfil do Gestor	Identificação do responsável pelos investimentos em TI e segurança da informação	4	e-mail, cargo, departamento, decisão de compra
Perfil da Empresa	Identificação da empresa e do parque de informática, nível de utilização dos recursos de TI	4	número de funcionários, qtde de computadores, responsabilidade pela área de TI
Ferramentas e Técnicas	Importância das ferramentas e técnicas de gestão da segurança da informação, se a empresa a possui	20	na sua empresa qual o grau de importância do uso do *firewall,* antivírus etc.
Fatores	Questiona sobre os fatores motivadores ou inibidores para adoção da gestão da segurança da informação	8	recomendação de um especialista externo ou fornecedor da área
TOTAL DE QUESTÕES		**36**	

Quadro 7: conjunto de variáveis

Este trabalho selecionou 20 controles dos 127 presentes na norma ISO/IEC 17799:2005 para serem pesquisados junto às pequenas e médias empresas. Dentre as 11 seções presentes, foi selecionado pelo menos um controle de cada seção, entretanto, em algumas seções mais de um controle se mostrou importante por sua possível aplicação nas empresas pesquisadas. As seções da norma onde foram selecionados mais de um controle são: Gestão de Ativos (2); Segurança Física e do Ambiente (2); Gestão das Operações e Comunicações (4); Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação (3); Conformidade (2).

A seleção dos controles baseou-se em pesquisas sobre segurança da informação realizadas pela Módulo Security no Brasil, pelo FBI nos Estados Unidos, pelas recomendações da norma ABNT NBR ISO/IEC 17799:2005, através de entrevistas preliminares realizadas com os gestores, além da experiência profissional do pesquisador. Os controles selecionados, bem como a fonte de pesquisa usada para cada um deles, encontra-se no anexo deste trabalho.

3.4 PROCEDIMENTOS PARA COLETA DE DADOS

Para a coleta de dados, o pesquisador realizou telefonemas diretamente ao gestor (nome e função disponibilizados no cadastro CIESP) explicando os motivos da pesquisa e pedindo suas respostas ou da pessoa responsável por aprovação de investimentos em gestão da segurança da informação. Após contato telefônico, foi

enviado e-mail reforçando o pedido e indicando o endereço do *web site* (www.professorvirtual.com.br/mestrado) em que o mesmo poderia responder ao questionário eletrônico.

3.5 PROCEDIMENTOS PARA ANÁLISE DOS RESULTADOS

Foram realizados procedimentos de estatística descritiva para verificação de significância dos dados através de procedimentos de amostragem, coleta e validação dos dados, utilizando o *software* Microsoft Excel e o *software* SPSS.

Buscou-se verificar a existência de relação positiva entre a adoção da gestão da segurança da informação e os seguintes fatores:

- tamanho da empresa – pequena ou média;
- quantidade de computadores em uso;
- existência de um departamento interno de TI;
- nível de informatização dos negócios da empresa.

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

A pesquisa foi realizada entre os meses de fevereiro e março de 2007. Foram contatadas por telefone as 256 empresas da amostra, sendo que destas:

- 165 aceitaram participar da pesquisa e foram encaminhadas informações por e-mail com o endereço eletrônico do questionário;
- 21 empresas desistiram de participar após receberem o e-mail e serem contatadas pela segunda vez;
- 43 empresas responderam ao questionário.

4.1 CARACTERIZAÇÃO DA AMOSTRA

Dentre as empresas que responderam ao questionário, a amostra ficou representada da seguinte forma:

- Quanto ao cargo que ocupa na empresa:

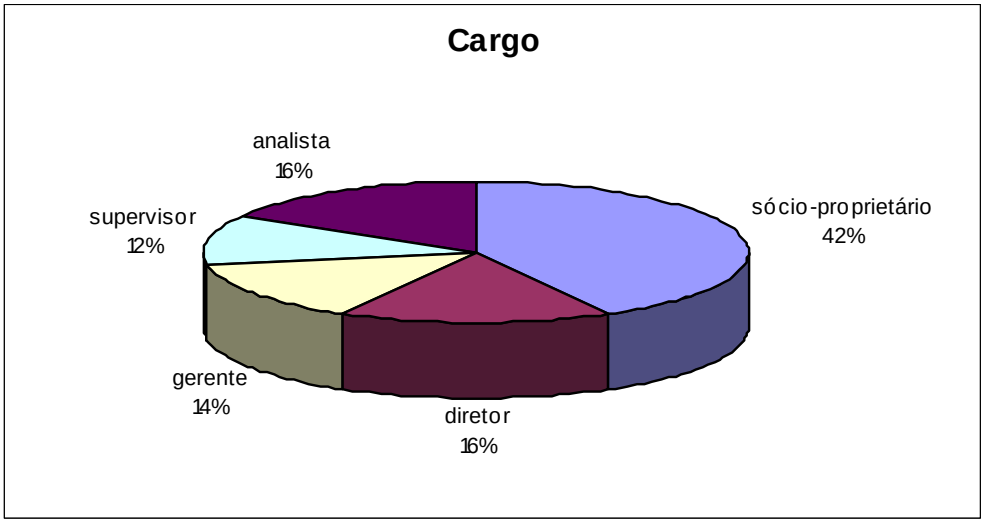

Gráfico 2: cargo

- Quanto ao departamento em que atua:

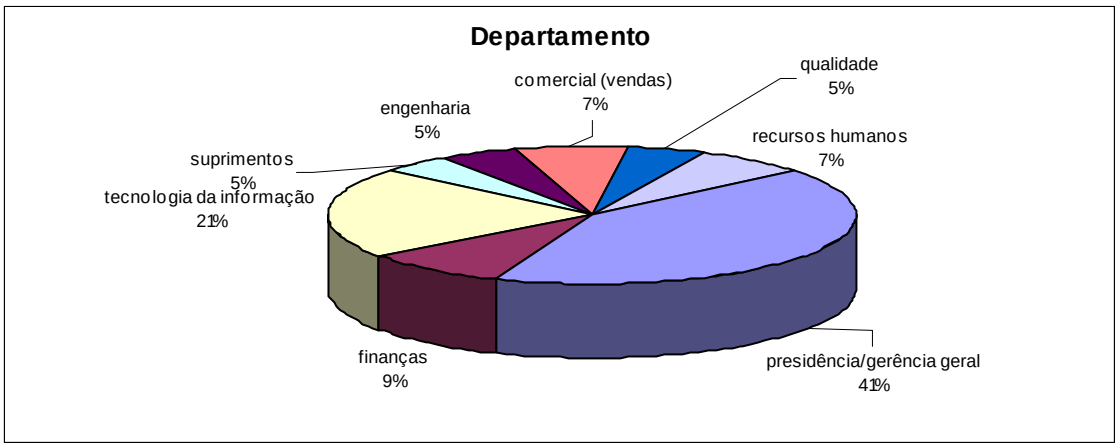

Gráfico 3: departamento

- Quanto à decisão de compra:

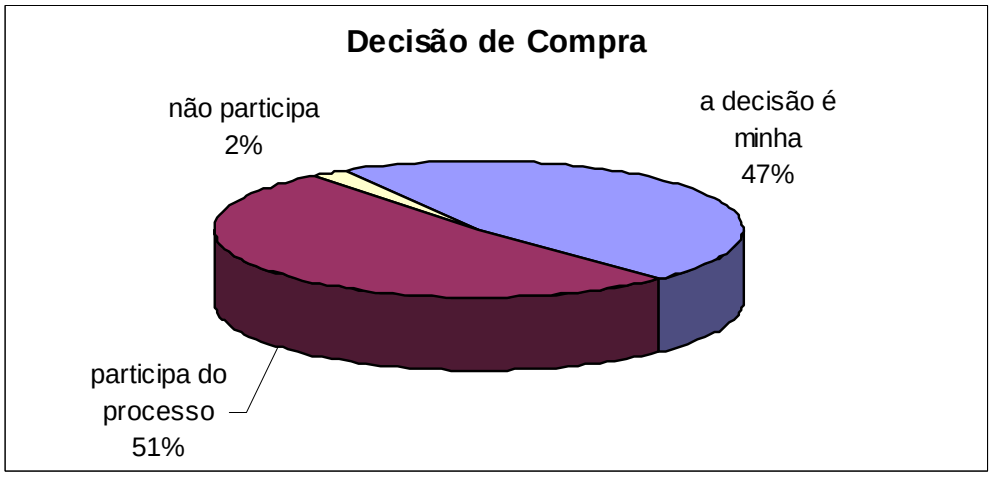

Gráfico 4: decisão de compra

Na amostra, 84% dos pesquisados ocupam cargos gerenciais ou acima, sendo: 12% supervisores, 14% gerentes, 16% diretores e a maioria são sócios-proprietários representando 42% dos pesquisados. Esses dados se confirmam na questão sobre o departamento de atuação onde 41% encontram-se na presidência ou gerência geral da empresa, seguidos em 21% pelo departamento de Tecnologia da Informação e 9% no departamento de Finanças.

Na amostra, 98% dos pesquisados possuem envolvimento sobre a decisão de compra de ferramentas e técnicas de gestão da segurança da informação ou TI.

Quanto às características das empresas respondentes em relação ao porte e ao número de empregados, a amostra coletada está representada da seguinte forma: 5% são micro-empresas (até 10 empregados), 81% são pequenas empresas (entre 10 e 99 funcionários) e 14% são médias empresas (de 100 a 499 funcionários). A delimitação da pesquisa inclui somente pequenas e médias empresas, assim as 5% consideradas micro-empresas serão excluídas da amostra para as análises das ferramentas/técnicas e fatores de adoção.

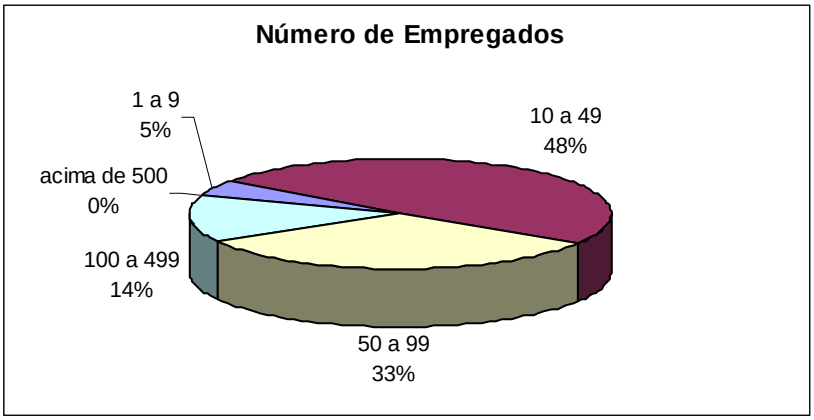

Gráfico 5: número de empregados

Quanto ao número de computadores, a maioria das empresas pesquisadas possui entre 5 e 100 computadores (72%), com maior concentração entre 10 a 20 computadores (28%).

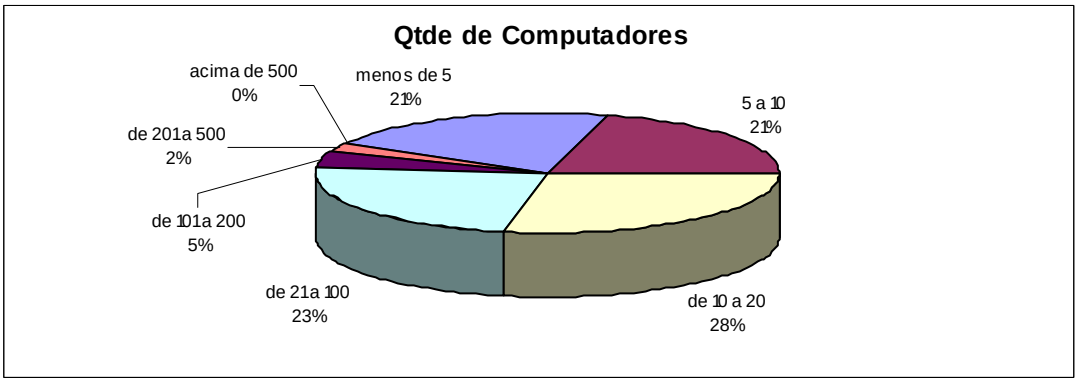

Gráfico 6: quantidade de computadores

A responsabilidade da área de TI na maioria das empresas da amostra é de um departamento interno ou funcionário (56%), enquanto os outros 44% são de empresas terceiras, sendo 23% com contrato e 21% contatadas por chamados eventuais.

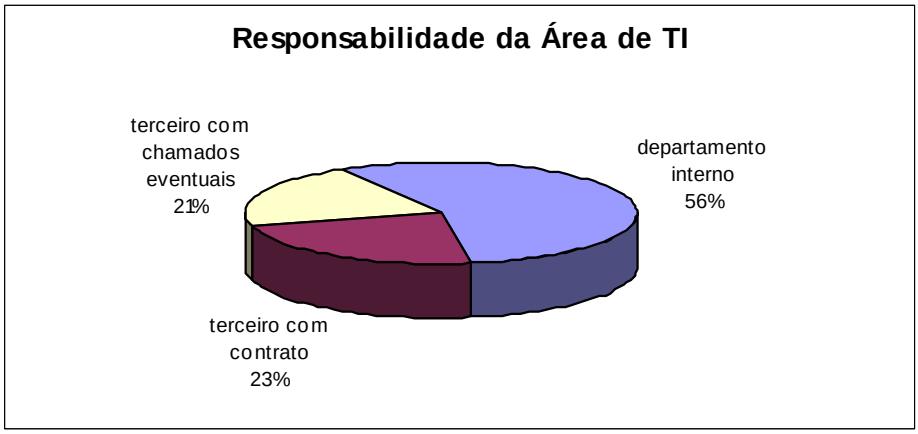

Gráfico 7: responsabilidade da área de TI

Quando perguntados sobre o nível de informatização de suas operações, a maioria das empresas o considerou entre médio (65%) e alto (28%) o que pode sugerir a necessidade de uma gestão de segurança da informação mais eficaz nessas empresas devido a maior concentração de informações em computadores.

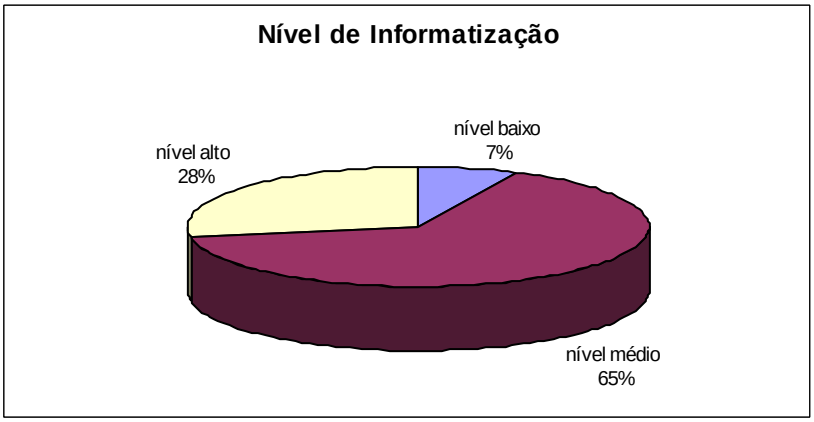

Gráfico 8: nível de informatização

Para ajudar as empresas pesquisadas a responder sobre o nível de informatização de suas operações, foram consideradas as seguintes proposições no questionário:

- **baixo:** uso constante de edição de documentos, e-mails, acesso a Internet;
- **médio:** as considerações do nível baixo, mais uso intensivo de planilhas eletrônicas e Internet Banking;
- **alto:** as considerações do nível médio, mais uso de sistema integrado, acesso remoto a funcionários/fornecedores, comércio eletrônico.

4.2 FERRAMENTAS E TÉCNICAS DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Os resultados apresentados a seguir, das ferramentas e técnicas de gestão da segurança da informação, foram divididos nas três camadas da gestão da segurança da informação: física, lógica e humana. A amostra foi purificada, sendo retiradas duas empresas, uma por não estar enquadrada como pequena ou média empresa definida neste trabalho e a outra porque respondeu não participar do processo de aquisição de ferramentas/técnicas de gestão de segurança da informação ou TI.

4.2.1 CAMADA FÍSICA

Nove questões foram formuladas para representar a camada física com base nas seções: Gestão das operações e comunicações, Segurança física e do ambiente, Controle de acesso, Gestão de incidentes de segurança da informação; presentes na norma ISO/IEC 17799:2005.

Tabela 2: camada física

FERRAMENTAS/TÉCNICAS	Média	Desvio	Possui	Não
Antivírus	**4,56**	**0,84**	**41**	**0**
Sistema de backup	4,46	1,03	40	1
Firewall	4,29	1,08	33	8
Equipamento para proteção de falhas na energia elétrica	3,73	1,53	34	7
Nome de usuário, senha individual e secreta para acesso a rede	3,68	1,44	33	8
Sala de servidores protegida e em local restrito	3,15	1,59	18	23
Descarte seguro da mídia removível	3,07	1,31	13	28
Monitoramento e análise crítica dos registros (*logs*)	3,07	1,25	13	28
Canais de comunicação para registro de eventos de segurança	2,83	1,14	16	25

Foi unânime para as empresas pesquisadas o uso do Antivírus como ferramenta/técnica de gestão da segurança da informação, tanto em grau de importância com média 4,59 e desvio padrão 0,84 quanto se possuem ou não, e 100% das empresas pesquisadas alegaram possuir. O fato pode ser atribuído aos históricos estragos causados em informações empresariais conseqüentes de vírus de computador como: *I Love You*, Melissa e Slamer. Além do conhecimento público do uso do antivírus e sua constante distribuição junto à venda de computadores novos, como parte integrante do pacote de *softwares* pré-instalados.

Sistema de *backup* ficou em segundo lugar em ordem de importância e de instalação, demonstrando a preocupação das empresas pesquisadas com a guarda e recuperação de informações importantes ao negócio no caso de qualquer fraude ou pane nos recursos de TI. *Firewall* aparece em terceiro lugar em ordem de importância e em quarto lugar quando ordenado pela coluna “possui ou não” a ferramenta/técnica de segurança. Em seu lugar, aparece Equipamento para proteção de falhas de energia elétrica (no-breaks), o que demonstra que as empresas reconhecem a importância do *Firewall* como uma ferramenta importante para proteção de suas redes na Internet, porém, a instalação de *no-breaks* possui um processo de implementação mais fácil e é mais elementar seu uso, afinal uma simples queda de energia elétrica pode fazer sentir seus efeitos.

Chamou atenção o baixo número de empresas que protegem o acesso a *console* de seus servidores (18 de 41 empresas), o que pode indicar que as empresas se sentem seguras internamente não considerando as pesquisas que alegam que o maior número de incidentes ocorre por culpa de funcionários da própria empresa. Também não existe em várias das empresas pesquisadas um monitoramento dos registros de segurança o que pode deixá-las sem qualquer informação sobre as fraudes em seu sistema, inclusive se o invasor não deixar rastros aparentes.

O gráfico 9 mostra a quantidade de empresas que possui ou não a ferramenta/técnica de gestão da segurança da informação na camada física.

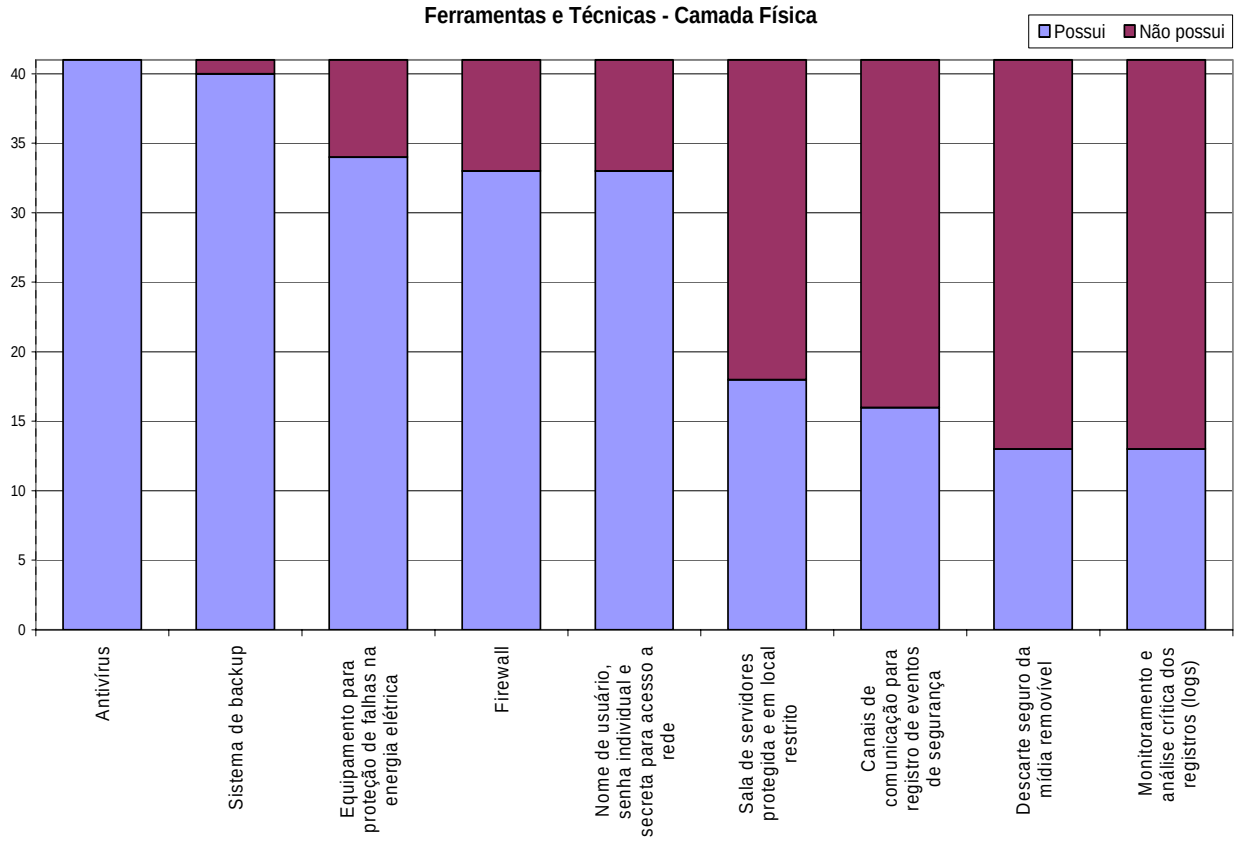

Gráfico 9: camada física

4.2.2 CAMADA LÓGICA

Na camada lógica, foram elaboradas três perguntas todas pertencentes à seção da norma ISO/IEC 17799:2005 - Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação.

Tabela 3: camada lógica

FERRAMENTAS/TÉCNICAS	Média	Desvio	Possui	Não
Atualização de software para correção de falhas de segurança	**3,56**	**1,32**	**27**	**14**
Criptografia em banco de dados e/ou para troca de informações	3,10	1,48	17	24
Supervisão do desenvolvimento terceirizado de software com requisitos para controles de segurança da informação	2,80	1,35	14	27

A ferramenta/técnica “Atualização de software para correção de falhas de segurança” foi a que apresentou maior média (3,56) e menor desvio padrão (1,32). Apesar de receber o primeiro lugar em relação às demais ferramentas/técnicas da camada lógica somente 65,85% das empresas pesquisadas possui implantadas,

uma porcentagem baixa de adesão, considerando que a ferramenta/técnica é disponibilizada gratuitamente na maioria dos sistemas operacionais atuais – como Windows XP – e *softwares* aplicativos – como Office, Photoshop, Acrobat. As vulnerabilidades presentes em *softwares* representam uma porta de entrada importante e muito usada por *hackers* de todo o mundo.

A pesquisa comprovou, conforme assevera Beal (2005), a baixa preocupação das empresas com o desenvolvimento do *software* terceirizado, podendo indicar a existência de um alto grau de confiança nos desenvolvedores e/ou nos produtos de *softwares* desenvolvidos por terceiros, ou uma despreocupação por parte das empresas.

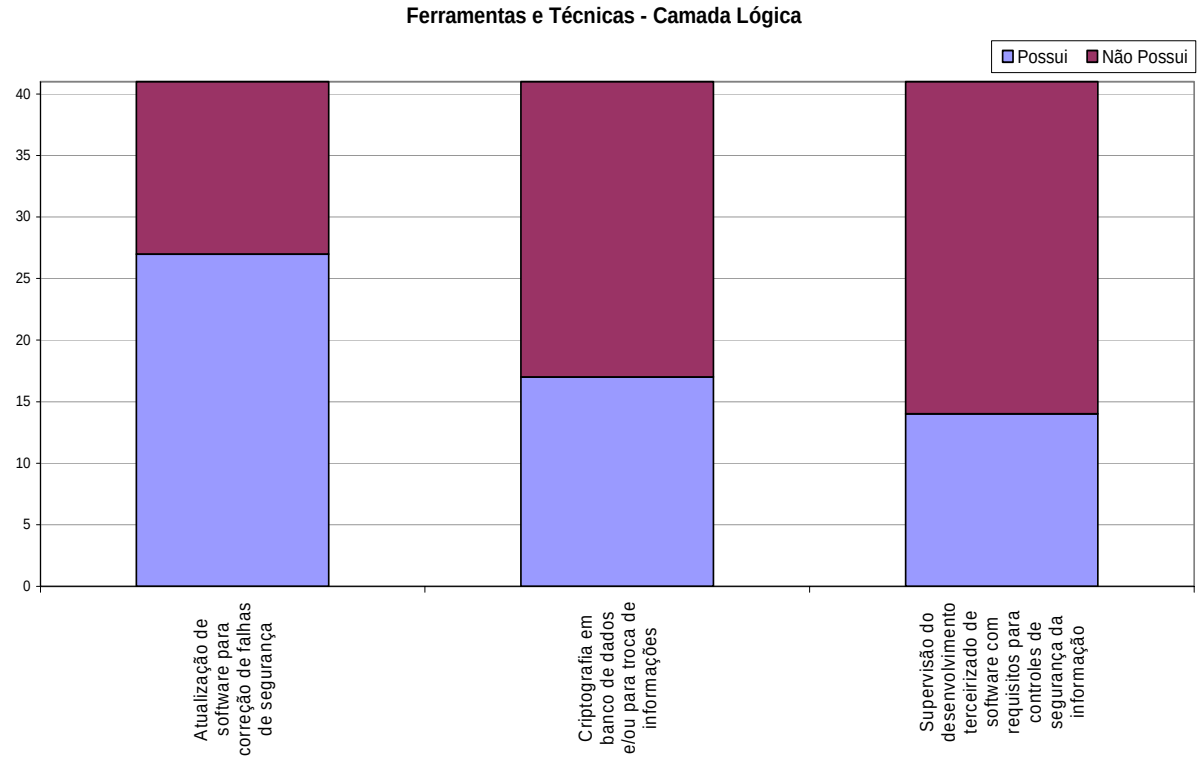

Gráfico 10: camada lógica

A criptografia é pouca usada ainda pelas pequenas e médias empresas, possivelmente devido à falta de conhecimento de seus benefícios. Com a possibilidade oferecida pelo governo de assinar digitalmente documentos como a declaração de renda, obter certidões da Receita Federal, cadastrar procurações e

acompanhar processos tributários eletronicamente, o uso da criptografia e dos certificados deve ganhar maior importância para as pequenas e médias empresas com o tempo, principalmente o uso do e-CPF e do e-CNPJ que são documentos eletrônicos vinculados aos números dos respectivos documentos físicos.

4.2.3 CAMADA HUMANA

A camada humana representa o maior desafio para a gestão da segurança da informação, devido à complexidade do elemento humano e às inúmeras variáveis presentes em seu comportamento. Nesta camada, oito questões enunciadas no questionário e extraídas das seções: Política de segurança da informação, Gestão de ativos, Organizando a segurança da informação, Segurança em Recursos Humanos e Gestão da continuidade do negócio da norma NBR ISO/IEC 17999:2005 tentaram conhecer a preocupação das empresas com essa camada e o que efetivamente está sendo feito.

Tabela 4: camada humana

FERRAMENTAS/TÉCNICAS	Média	Desvio	Possui	Não
Regras para uso da informação e dos recursos de TI	**3,68**	**1,19**	**26**	**15**
Controle dos direitos de propriedade intelectual	3,49	1,36	25	16
Aviso aos usuários sobre o monitoramento dos recursos de TI	3,39	1,43	24	17
Contratos com terceiros com termos claros relativos a segurança	3,32	1,46	18	23
Política de segurança da informação	3,24	1,34	19	22
Classificação da informação	3,17	1,26	19	22
Conscientização, educação e treinamento em segurança	2,95	1,30	15	26
Plano de recuperação de desastres e contingência	2,88	1,44	16	25

A ferramenta/técnica “Regras para uso da informação e dos recursos de TI” foi a que apresentou a maior média (3,68) e menor desvio padrão (1,19). Trata-se de um controle fácil de ser implementando por ser um documento (na maioria das vezes com apenas uma folha) com as normas de uso da informação assinados pelos funcionários e em algumas empresas fazem parte do próprio regulamento interno. É complementado pela ferramenta/técnica “Aviso aos usuários sobre o monitoramento dos recursos de TI”. Porém, para efetividade desses dois controles, é

necessário que ferramentas/técnicas sejam implantadas para o monitoramento dos usuários. Das nove ferramentas/técnicas pesquisadas na camada física, o “Monitoramento e análise crítica dos registros (*logs*) de auditoria” ficou em oitavo lugar e somente 31,7% das empresas pesquisadas alegaram possuir, o que demonstra que, apesar das pequenas e médias empresas se preocuparem em definir regras de uso dos recursos de TI e avisar aos usuários sobre o monitoramento, pouco se monitora efetivamente.

“Controle dos direitos de propriedade intelectual” ficou classificado em segundo lugar em grau de importância na camada humana, com média de 3,49 e desvio padrão 1,36. O conhecimento das leis que protegem os direitos autorais de *software*, por parte das empresas, e suas penalidades podem explicar a resposta.

Outra ferramenta/técnica de fácil implantação e que pode representar um ganho na gestão de segurança da informação de pequenas e médias empresas é a “Conscientização, educação e treinamento em segurança” dos empregados e terceiros, porém apresentou baixo grau de importância para as empresas e pouca adesão à implantação.

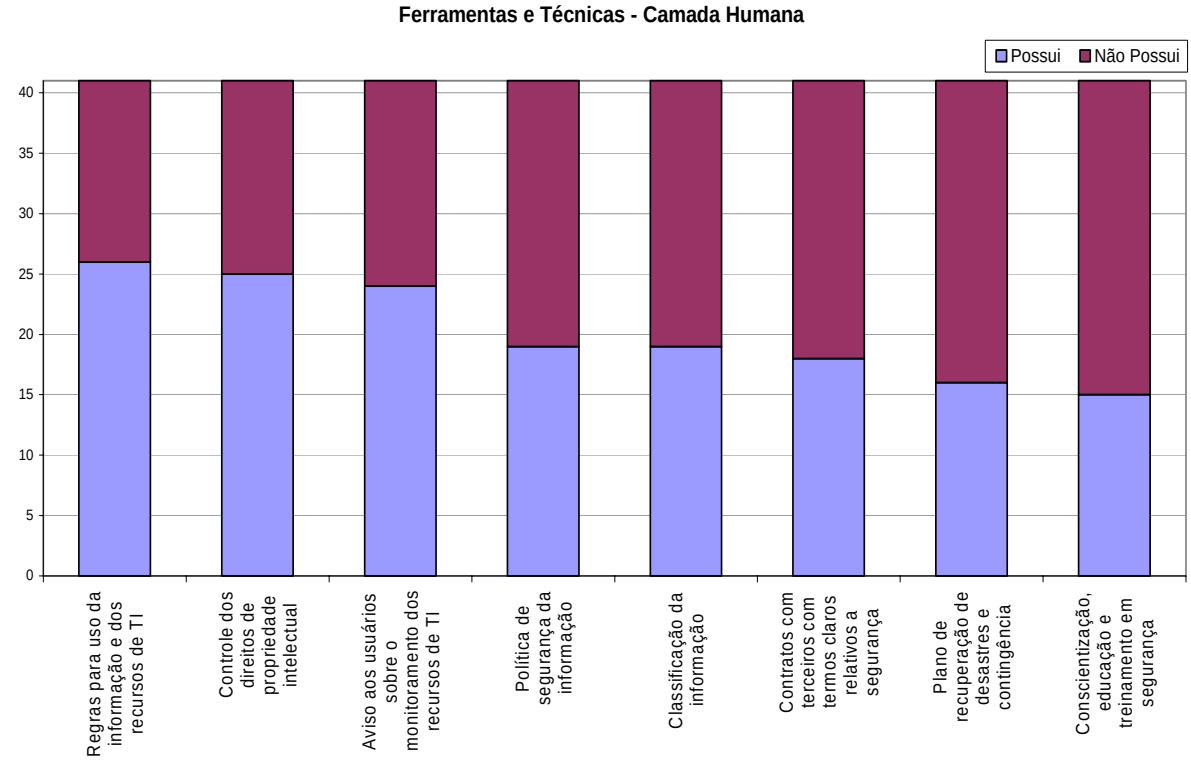

Gráfico 11: camada humana

Se observarmos os gráficos de adesão das três camadas: física, lógica e humana pelas empresas pesquisadas, percebe-se que a camada humana, devido ao número de ferramentas/técnicas, é a que apresenta maior carência de cuidados por parte dos administradores. Esta constatação confirma as alegações de Schneier (2001) e as preocupações de Fontes (2006).

O interessante é que muitas das ferramentas/técnicas listadas neste trabalho na camada humana não são de difícil implementação, requerem na maioria dos casos baixo investimento em ferramentas computacionais e tempo e dedicação da gerência. O que confirma as considerações de Sêmola (2003) quando diz que as empresas se preocupam mais com os aspectos tecnológicos da segurança da informação do que com os aspectos físicos e humanos.

O próximo gráfico representa o grau de importância atribuído a todas as ferramentas ou técnicas de gestão da segurança da informação independente da camada a que foi categorizado:

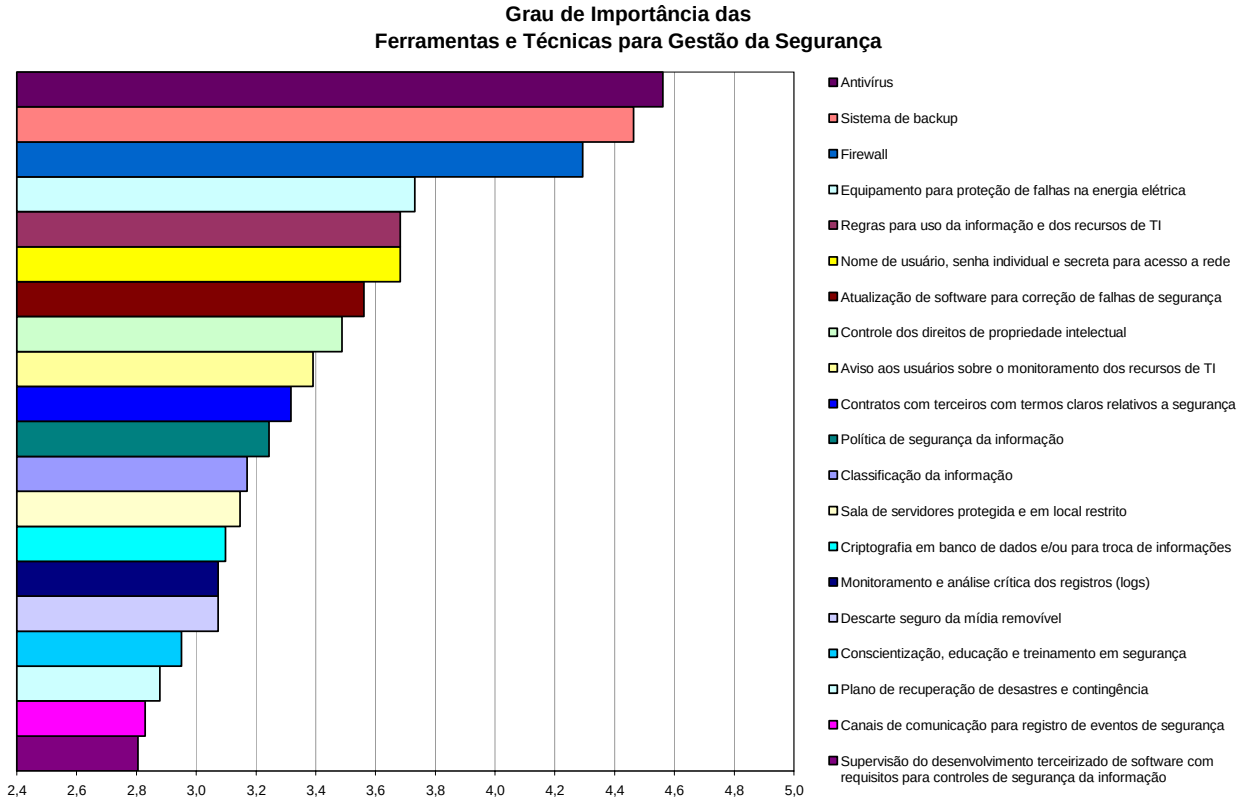

Gráfico 12: grau de importância das ferramentas/técnicas

O gráfico confirma alguns dados reportados na 9ª Pesquisa Nacional de Segurança de Informação realizada pela empresa Módulo *Security* em outubro de 2003 e da pesquisa *Computer Crime and Security Survey* realizada em 2005 pelo *Computer Security Institute* (CSI) e pelo *Federal Bureau Investigation* (FBI) nos Estados Unidos, que apresentam que a maior ameaça e causa de perda de dinheiro com fraudes pelas empresas são os vírus de computador. Este fato justifica o grau de importância ser tão elevado também para pequenas e médias empresas. As ferramentas/técnicas Sistema de *Backup* e *Firewall*, respectivamente consideradas segunda e terceira mais importantes, também coincidem com a pesquisa da empresa Módulo e diferem da pesquisa do CSI/FBI que aponta em ordem de importância, as seguintes ferramentas/técnicas: *Firewall*, Antivírus e Sistema de Detecção de Intrusos (o último item não foi considerado nesta pesquisa por não ser de uso comum em pequenas e médias empresas).

As entrevistas realizadas com gestores para criação do questionário eletrônico também confirmam o grau de importância apontado na pesquisa, ao indicar o Antivírus, Backup e o *Firewall* como as principais ferramentas/técnicas citadas.

A implementação de uma Política de Segurança da Informação ficou em 11º lugar entre as 20 ferramentas/técnicas pesquisadas, uma posição modesta perante a importância que vários autores estudados e a norma NBR ISO/IEC 17799:2005 atribuem à ferramenta. Este fato indica que a maioria das pequenas e médias empresas investem e se preocupam com ferramentas/técnicas de uso pontual e ignoram ou esquecem o gerenciamento correto da segurança da informação enquanto atividade administrativa.

Em último lugar em grau de importância aparece “Supervisão do desenvolvimento terceirizado de software com requisitos para controles de segurança da informação” uma preocupação alegada por Beal (2005) para a implantação da gestão da segurança da informação nas empresas, mas como indica a pesquisa, não recebe a devida importância por parte das empresas.

4.3 GESTÃO DA SEGURANÇA DA INFORMAÇÃO NAS TRÊS CAMADAS

A fim de avaliar o nível de gestão da segurança da informação implementadas nas pequenas e médias empresas pesquisadas e conseqüentemente sua adequação a alguns itens da norma ISO/IEC 17799:2005, foi desenvolvida a seguinte metodologia:

a) verificar se a empresa possui pelo menos uma ferramenta/técnica instalada em cada uma das camadas de segurança: física, lógica e humana;

b) verificar se a porcentagem das ferramentas/técnicas que a empresa possui instalada é maior ou igual a 50%, independente da camada de segurança;

c) caso a empresa atenda às condições determinadas no item a e b, sua gestão da segurança da informação é classificada como satisfatória, caso contrário é classificada como insatisfatória.

O gráfico 13 mostra que a maioria das empresas pesquisadas (59%) se enquadrou no nível satisfatório, o que indica que existe uma preocupação da maioria das empresas com as três camadas da segurança.

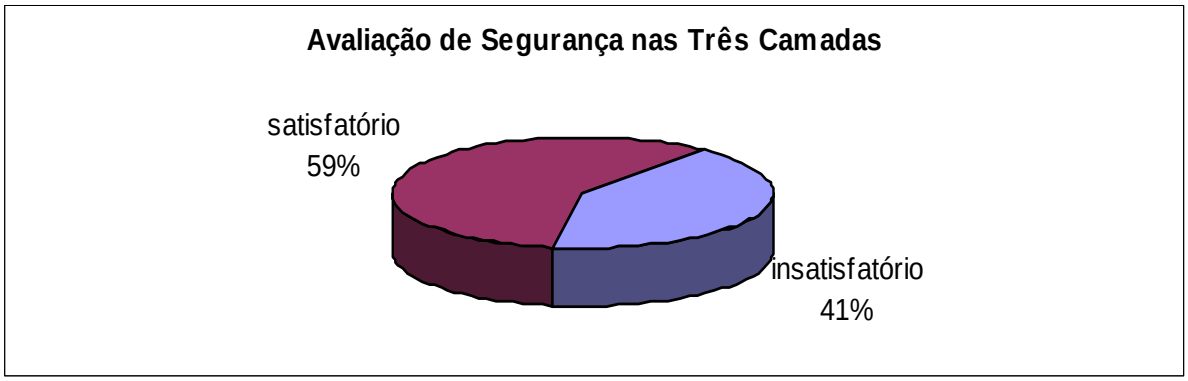

Gráfico 13: avaliação de segurança nas três camadas

O gráfico 14 representa a distribuição das ferramentas/técnicas instaladas nas empresas pesquisadas. A maior distribuição de freqüência encontrada está no intervalo entre 60% a 80% das ferramentas/técnicas instaladas, com 13 empresas. Acima de 80% encontram-se 9 empresas. Somando as duas freqüências, temos que 53,7% das empresas pesquisadas possuem mais que 60% das ferramentas/técnicas

instaladas o que pode inferir que a maioria encontram-se adequadas a gestão da segurança da informação independente da camada.

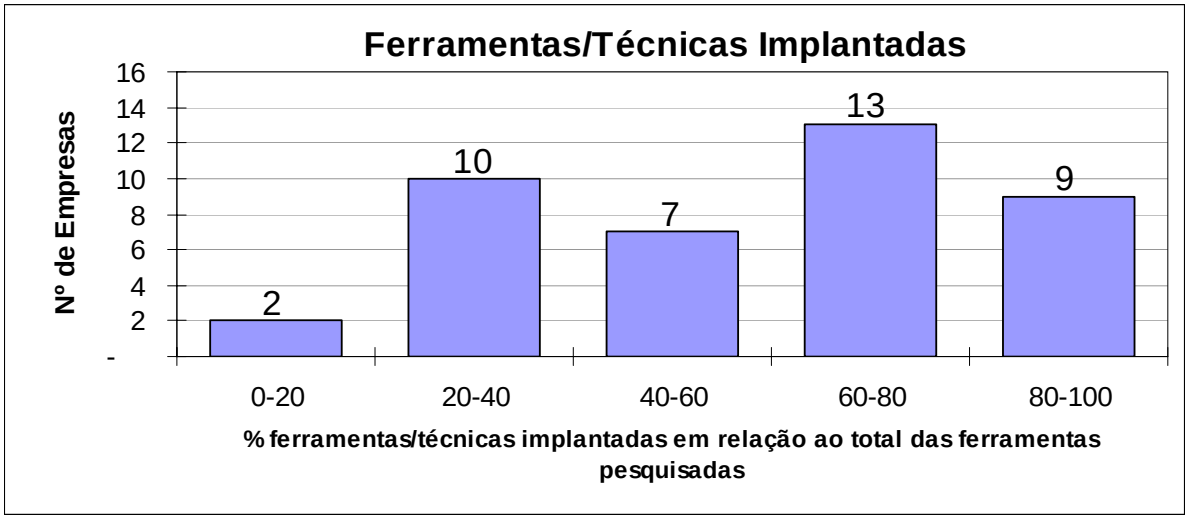

Gráfico 14: quantidade de ferramentas/técnicas implantadas, por faixa, nas 43 empresas pesquisadas

Ao diferenciar as pequenas empresas das médias empresas, pôde-se observar que somente em uma das médias empresas a gestão da segurança da informação foi categorizada como insatisfatória, pois não atende aos requisitos mínimos estabelecidos. Todas as demais consideradas insatisfatórias são representadas por pequenas empresas, por possuírem menos recursos financeiros e humanos acabam não conseguindo atender às três camadas efetivamente. Ao analisar o gráfico 15, percebe-se que as pequenas empresas possuem mais ferramentas/técnicas instaladas do que as médias empresas, isso deve-se ao fato do pequeno número de médias empresas que responderam a pesquisa.

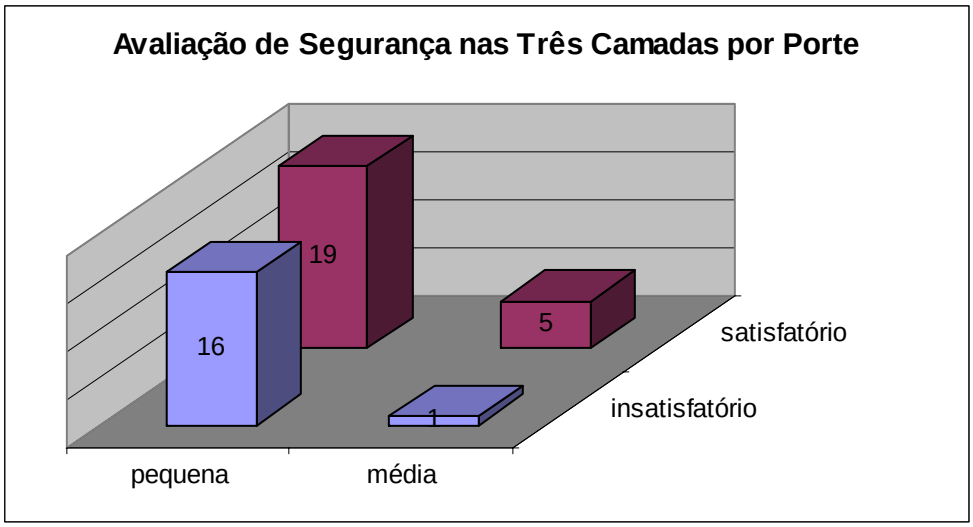

Gráfico 15: avaliação de segurança nas três camadas por porte de empresa

As principais ferramentas ou técnicas que as pequenas e médias empresas não possuem implantadas e que merecem maior atenção de seus administradores são:

Tabela 5: principais ferramentas ou técnicas que as empresas não possuem implantadas

Camada de Segurança	Ferramenta ou Técnica	% de empresas que não possui
Física	Descarte seguro da mídia removível	68%
	Monitoramento e análise crítica dos registros (logs)	68%
	Canais de comunicação para registro de eventos de segurança	61%
Lógica	Supervisão do desenvolvimento terceirizado de software com requisitos para controles de segurança da informação	66%
	Criptografia em banco de dados e/ou para troca de informações	59%
Humana	Conscientização, educação e treinamento em segurança	63%
	Plano de recuperação de desastres e contingência	61%
	Contratos com terceiros com termos claros relativos à segurança	56%

4.4 ADERÊNCIA ÀS SEÇÕES DA NORMA ISO 17799

A próxima análise verifica a porcentagem das ferramentas/técnicas de gestão da segurança da informação que as empresas pesquisadas possuem implantadas em relação a cada seção da norma ISO/IEC 17799:2005. Nas seções em que existiam mais de uma ferramenta/técnica abordada pela pesquisa, foi efetuada uma média aritmética simples.

Tabela 6: aderência às seções da norma ISO 17799

Seção da Norma	Ferramenta ou Técnica Pesquisada	Média	Porcentagem
Política de Segurança da Informação	Política de segurança da informação	3,24	46%
Organizando a Segurança da Informação	Contratos com terceiros com termos claros relativos à segurança	3,32	44%
Gestão de Ativos	Regras para uso da informação e dos recursos de TI	3,68	55%
	Classificação da informação	3,17	
Segurança em Recursos Humanos	Conscientização, educação e treinamento em segurança	2,95	37%
Segurança Física e do Ambiente	Equipamento para proteção de falhas na energia elétrica	3,73	63%
	Sala de servidores protegida e em local restrito	3,15	
Gestão das Operações e Comunicações	Antivírus	4,56	68%
	Sistema de *backup*	4,46	
	Firewall	4,29	
	Descarte seguro da mídia removível	3,07	
	Monitoramento e análise crítica dos registros (*logs*)	3,07	
Controle de Acesso	Nome de usuário, senha individual e secreta para acesso à rede	3,68	80%
Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação	Atualização de software para correção de falhas de segurança	3,56	47%
	Criptografia em banco de dados e/ou para troca de informações	3,10	
	Supervisão do desenvolvimento terceirizado de software com requisitos para controles de segurança da informação	2,80	
Gestão de Incidentes de Segurança da Informação	Canais de comunicação para registro de eventos de segurança	2,83	39%
Gestão da Continuidade de Negócio	Plano de recuperação de desastres e contingência	2,88	39%
Conformidade	Controle dos direitos de propriedade intelectual	3,49	60%
	Aviso aos usuários sobre o monitoramento dos recursos de TI	3,39	

A seção que apresenta maior aderência por parte das pequenas e médias empresas é a Controle de Acesso, com 80%, seguida por Gestão das Operações e Comunicações (68%) e por Segurança Física e do Ambiente (63%). Comprovando

novamente as considerações de Sêmola (2003) sobre a preocupação das empresas com os aspectos tecnológicos da gestão da segurança da informação e o esquecimento de outros aspectos importantes.

Cabe dizer que a intenção desta análise não é verificar se a empresa pode ser certificada ou não pela norma, pois as informações aqui apresentadas são respostas às percepções e ao conhecimento do respondente. Para verificar a correta adequação da empresa aos requisitos da norma, faz-se necessário um acompanhamento *in loco* dos controles implantados.

4.5 FATORES MOTIVADORES E INIBIDORES

Além de levantar as principais ferramentas e técnicas utilizadas pelas pequenas e médias empresas pesquisadas, este trabalho através de sua pergunta problema verificou os fatores motivadores e inibidores para uso e aplicação da gestão da segurança da informação, pesquisando os seguintes fatores:

- **Motivadores:**
    - Recomendação de um especialista externo ou fornecedor da área;
    - Incidente de segurança ocorrido anteriormente;
    - Consciência do próprio gestor (no sentido do mesmo conhecer a importância das ferramentas/técnicas para a adoção da gestão da segurança da informação);
    - Para evitar possíveis perdas financeiras ou operacionais.
- **Inibidores:**
    - Valor do investimento;
    - Dificuldade em mensurar a relação custo/benefício do investimento;
    - Falta de conhecimentos sobre ferramentas ou técnicas de defesa;
    - Cultura organizacional.

A média com o grau de importância de cada fator, desvio padrão e erro amostral calculado para um nível de confiança de 95% encontra-se na tabela 7.

Tabela 7: fatores motivadores e inibidores

Fatores		Amostra				
		média	**σ**	**erro amostral**	**limite superior**	**limite inferior**
motivadores	especialista externo	3,51	1,12	0,35	3,87	3,16
	incidente anterior	3,34	1,24	0,39	3,73	2,95
	consciência do gestor	3,63	1,13	0,36	3,99	3,28
	evitar perdas financeiras	**4,37**	**0,83**	**0,26**	**4,63**	**4,10**
inibidores	valor do investimento	3,66	1,13	0,36	4,02	3,30
	relação custo/ benefício	3,37	1,13	0,36	3,72	3,01
	falta de conhecimento	**3,71**	**1,15**	**0,36**	**4,07**	**3,35**
	cultura organizacional	3,66	1,02	0,32	3,98	3,34

Para verificar a significância das médias apresentadas na tabela 7, foram realizados os seguintes testes com o uso do *software* SPSS versão 13.0:

1. teste *Shapiro-Wilk* para verificar a normalidade dos dados;
2. teste *Kruskal-Wallis* para verificar a significância entre as médias;
3. teste *Mann-Whitney* para verificar a média que apresentava maior significância;

O teste *Shapiro-Wilk* revelou um valor de $p < 0,0001$, para tanto a distribuição não pode ser considerada normal, o que inviabilizou o uso de testes paramétricos como ANOVA – *Analysis of Variance*. Assim, procedeu-se ao uso de testes não-paramétricos.

O teste *Kruskal-Wallis* realizado com as médias dos fatores motivadores e com as médias dos fatores inibidores revelou que em fatores motivadores nem todas as médias são iguais estatisticamente ($p < 0,0001$), porém as médias dos fatores inibidores não apresentaram diferenças significativas entre si ($p = 0,429$), ao nível de confiança de 95%, o que pode inferir que todos os fatores inibidores têm a mesma importância para a amostra de empresas pesquisadas.

Para confirmar entre os fatores motivadores a média que apresentava diferença significativa foi realizado o teste *Mann-Whitney*, comparando a média de cada fator entre si. Os resultados estão apresentados na tabela 8:

Tabela 8: teste *Mann-Whitney*

Fatores Motivadores	*Mann-Whitner U*	*Wilcoxon W*	*Z*	*Asymp.Sig (2-tailed)*
especialista interno x incidente anterior	773,000	1634,000	-0,648	0,517
especialista interno x consciência do gestor	775,500	1636,500	-0,626	0,531
especialista interno x evitar perdas financeiras	482,000	1343,000	-3,529	0,000
incidente anterior x evitar perdas financeiras	443,500	1304,500	-3,870	0,000
consciência do gestor x evitar perdas financeiras	529,000	1390,000	-3,061	0,002

A coluna *Asymp. Sig (2-tailed)* da tabela 8, representa o valor de p para cada análise. Dentre as médias analisadas a que apresentou diferença significativa entre as demais foi a do fator “evitar perdas financeiras”, com $p < 0,05$, inferindo que o fator motivador para as empresas implantarem ferramentas/técnicas de gestão da segurança da informação se dá principalmente para evitar possíveis perdas financeiras ou operacionais.

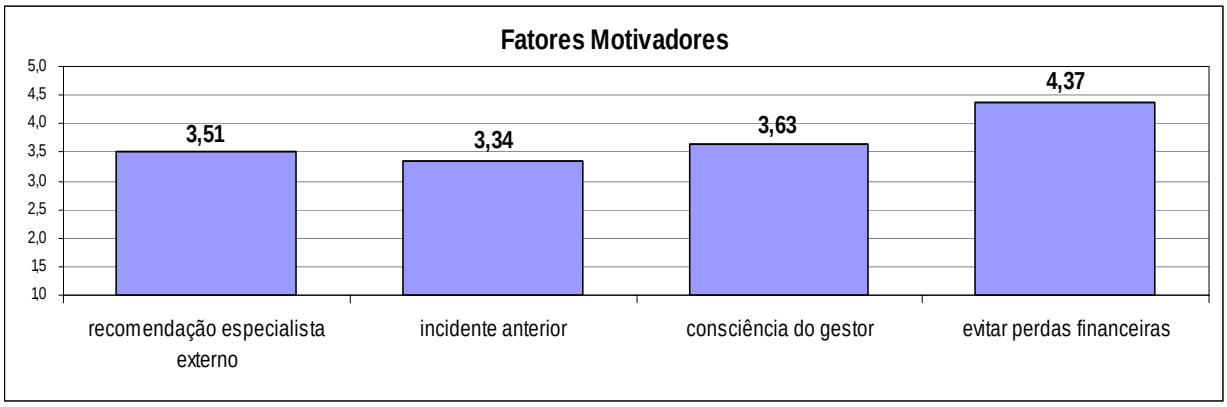

Gráfico 16: fatores motivadores

Apesar dos testes estatísticos revelarem que os demais fatores motivadores têm a mesma significância em termos de média, o fator “consciência do gestor” (segunda maior média) merece atenção por indicar certa incoerência com os fatores inibidores que mostram a “falta de conhecimento” com a maior média, pois é estranho identificar que o gestor tem consciência dos perigos que sua empresa corre com relação às informações, porém não se preocupa em ter o conhecimento adequado para sanar os problemas. Fato que também ficou claro nas entrevistas preliminares.

Nas entrevistas realizadas para criação do questionário ficou evidenciado que incidentes anteriores tinham um peso considerável na adoção de gestão da

segurança da informação, assim como pesquisado por Gabbay (2003), porém nesta pesquisa não se apresentou como fator importante, o que pode indicar que as pequenas e médias empresas não têm sofrido incidentes de segurança da informação como apontado por Gupta e Hammond (2004) ou não têm monitorado (como apresenta o baixo grau de importância nas ferramentas/técnicas no item anterior) seus recursos para descobrir evidências de ataques aos ativos de informação, o que pode representar um sério risco a continuidade do negócio e/ou vazamento de segredos industriais e processos a concorrentes.

A importância da recomendação de um especialista externo ou fornecedor da área também ficou clara nas entrevistas e foi apontada nas pesquisas sobre adoção de TI de Cragg e King (1993) e Thong. Porém não apresentou média significativa como fator motivador na adoção de gestão da segurança da informação na amostra pesquisada.

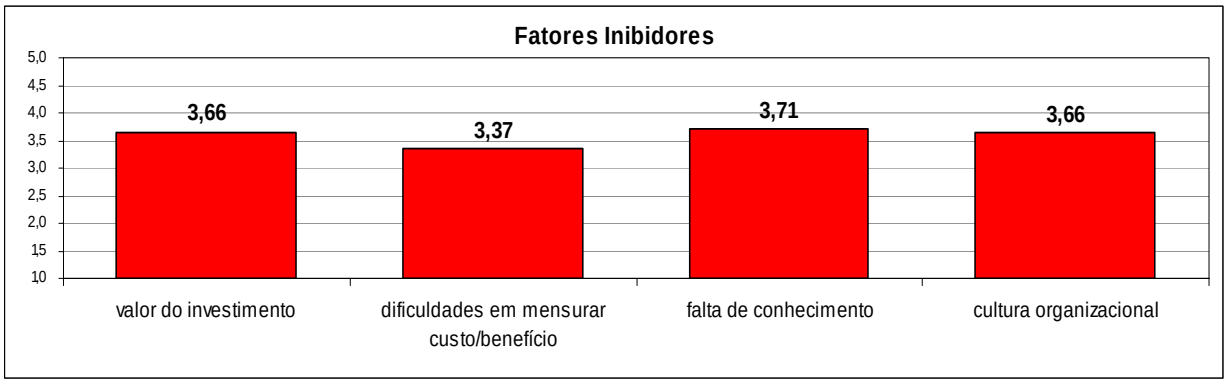

Gráfico 17: fatores inibidores

Nos fatores inibidores não é possível destacar o mais importante, visto as médias encontradas não apresentarem diferenças significativas. Porém, de acordo com as entrevistas preliminares a falta de conhecimento do gestor é um fator inibidor que merece certa atenção, pois ficou explícito nas entrevistas que não existe uma preocupação dos gestores em se manterem informados sobre assuntos ligados à gestão da segurança. Em relação aos outros fatores inibidores, conclui-se que para as empresas pesquisadas o valor do investimento e sua mensuração em razão do custo/benefício não são dispendiosos e portanto fáceis de serem aprovados no orçamento e implementados quando a questão é segurança da informação. A cultura organizacional também não mereceu destaque entre os fatores inibidores, possivelmente pela crescente divulgação de notícias relacionadas a incidentes de

segurança da informação na mídia em geral, e a conseqüente conscientização das pessoas com relação à mesma.

Conforme proposto no item 3.5 Procedimentos para Análise de Resultados, buscou-se verificar a existência de relação positiva entre a adoção da gestão da segurança da informação e os seguintes itens:

- tamanho da empresa – pequena ou média;
- quantidade de computadores em uso;
- existência de um departamento interno de TI;
- nível de informatização dos negócios da empresa;

Para tanto, a amostra foi dividida em grupos conforme as particularidades acima e analisado cada caso para verificar a influência na adoção da gestão de segurança da informação.

4.5.1 ÁREA DE TI INTERNA

Tabela 9: área de TI interna

Fatores		Amostra		TI Interna	
		média	σ	média	σ
motivadores	especialista externo	3,51	1,12	3,50	1,29
	incidente anterior	3,34	1,24	3,17	1,34
	consciência do gestor	3,63	1,13	3,63	1,21
	evitar perdas financeiras	**4,37**	**0,83**	**4,33**	**0,92**
inibidores	valor do investimento	3,66	1,13	**3,67**	**1,24**
	relação custo/ benefício	3,37	1,13	3,29	1,16
	falta de conhecimento	**3,71**	**1,15**	3,46	1,32
	cultura organizacional	3,66	1,02	3,58	1,14

O teste *Kruskal-Wallis* foi realizado para verificar a significância das médias dos fatores motivadores e inibidores nas empresas que responderam possuir a área de TI interna e resultou um $p = 0,011$ para os fatores motivadores e $p = 0,711$ para os fatores inibidores, indicando que somente em fatores motivadores é possível determinar um fator relevante pois o valor de p é menor que 0,05. A tabela 10 exibe os resultados do teste *Mann-Whitney* com os dados das empresas que possuem departamento interno de TI, confirmando os resultados da amostra total que o único fator motivador que possui média significativa é “evitar perdas financeiras”.

Tabela 10: teste *Mann-Whitney – Área de TI interna*

Fatores Motivadores	*Mann-Whitner U*	*Wilcoxon W*	*Z*	*Asymp.Sig (2-tailed)*
especialista interno x incidente anterior	244,500	544,500	-0,923	0,356
especialista interno x consciência do gestor	272,500	572,500	-0,330	0,741
especialista interno x evitar perdas financeiras	180,500	480,500	-2,386	0,017
incidente anterior x evitar perdas financeiras	141,000	441,000	-3,178	0,001
consciência do gestor x evitar perdas financeiras	189,000	489,000	-2,174	0,030

Nos fatores inibidores, assim como na amostra total, não foi possível determinar o mais importante, mas percebe-se uma diferença matemática nas médias da amostra total em relação à amostra das empresas que possuem a área de TI, migrando a maior média do fator inibidor “falta de conhecimento” para “valor do investimento”. Porém devido aos testes estatísticos realizados e a influência do

pequeno tamanho da amostra não foi possível indicar a influência do departamento de TI em recomendar ou sugerir ferramentas e técnicas para gestão da segurança da informação.

Os gráficos 18 e 19 exibem as médias da amostra total em relação à amostra das empresas que possuem o departamento interno de TI.

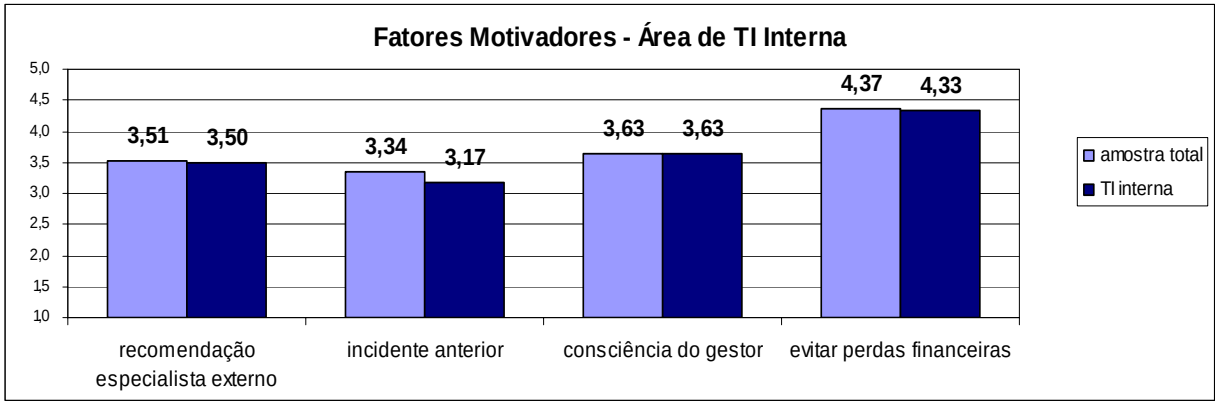

Gráfico 18: fatores motivadores com a existência da área de TI interna

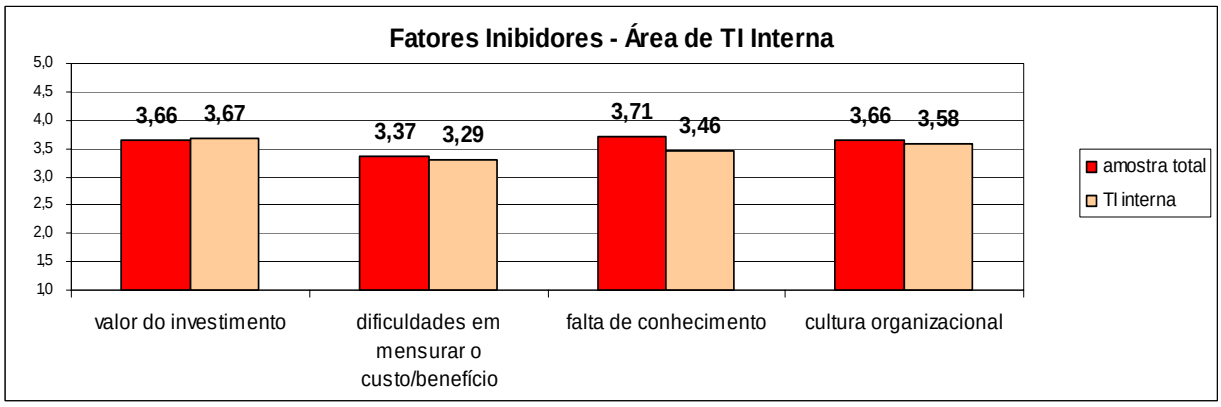

Gráfico 19: fatores inibidores com a existência da área de TI interna

4.5.2 TAMANHO DA EMPRESA

Tabela 11: tamanho da empresa

Fatores		Amostra		Pequena		Média	
		média	σ	média	σ	média	σ
motivadores	especialista externo	3,51	1,12	3,51	1,17	3,50	0,84
	incidente anterior	3,34	1,24	3,26	1,20	3,83	1,47
	consciência do gestor	3,63	1,13	3,60	1,14	3,83	1,17
	evitar perdas financeiras	**4,37**	**0,83**	**4,31**	**0,83**	**4,67**	**0,82**
inibidores	valor do investimento	3,66	1,13	3,54	1,15	**4,33**	**0,82**
	relação custo/ benefício	3,37	1,13	3,37	1,19	3,33	0,82
	falta de conhecimento	**3,71**	**1,15**	3,63	1,19	4,17	0,75
	cultura organizacional	3,66	1,02	**3,63**	**1,00**	3,83	1,17

Outra verificação feita foi à comparação entre os resultados obtidos na amostra total com os obtidos nos grupos porte da empresa: pequeno ou médio. Novamente executaram-se os testes estatísticos *Kruskal Wallis* e *Mann-Whitney* para verificar se a diferença matemática apresentada nas médias da tabela 11 era significativa estatisticamente.

Tabela 12: teste *Kruskal Wallis – Tamanho da Empresa*

porte	*valor de p fatores motivadores*	*valor de p fatores inibidores*
pequena empresa	0,001	0,675
média empresa	0,253	0,254

Tabela 13: teste *Mann-Whitney – Pequena Empresa*

Fatores	*Mann-Whitner U*	*Wilcoxon W*	*Z*	*Asymp.Sig (2-tailed)*
especialista interno x incidente anterior	540,000	1170,00	-0,880	0,379
especialista interno x consciência do gestor	579,00	1209,00	-0,408	0,683
especialista interno x evitar perdas financeiras	375,00	1005,00	-2,945	0,003
incidente anterior x evitar perdas financeiras	306,500	936,500	-3,752	0,000
consciência do gestor x evitar perdas financeiras	393,500	1023,500	-2,713	0,007

A tabela 12 revela que somente na amostra de pequenas empresas em fatores motivadores existia diferença significativa entre as médias ($p < 0,05$). A

tabela 13 exibe os resultados dos testes efetuados com essa amostra, indicando novamente o fator “evitar perdas financeiras”.

Os gráficos 20 e 21 exibem a comparação entre as médias da amostra total em relação à amostra das empresas por tamanho/porte – pequena e média.

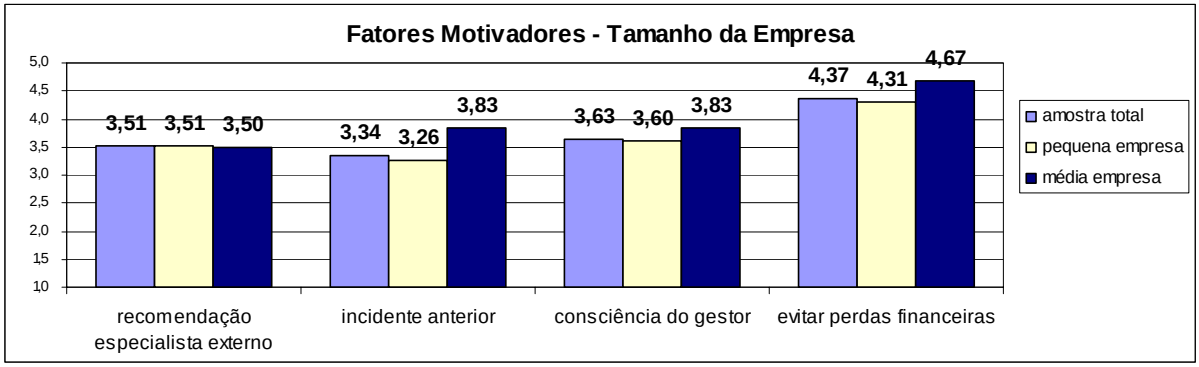

Gráfico 20: fatores motivadores de acordo com o tamanho da empresa

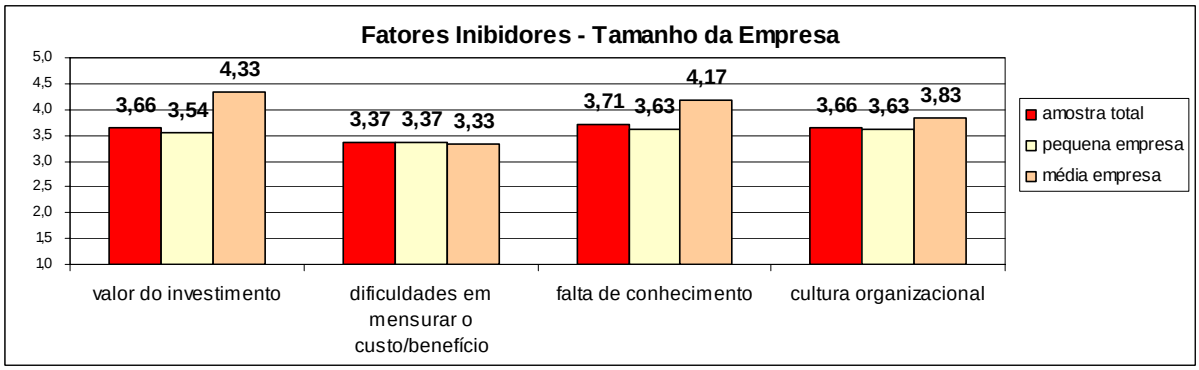

Gráfico 21: fatores inibidores de acordo com o tamanho da empresa

4.5.3 QUANTIDADE DE COMPUTADORES

Tabela 14: quantidade de computadores

Fatores		Amostra		Até 10 micros		De 11 a 20		Acima de 20	
		média	σ	média	σ	média	σ	média	σ
motivadores	especialista externo	3,51	1,12	3,59	1,23	3,83	1,19	3,08	0,79
	incidente anterior	3,34	1,24	3,24	1,25	3,58	1,24	3,25	1,29
	consciência do gestor	3,63	1,13	3,24	1,25	4,00	0,95	3,83	1,03
	evitar perdas financeiras	**4,37**	**0,83**	**4,06**	**0,90**	**4,50**	**0,67**	**4,67**	**0,78**
inibidores	valor do investimento	3,66	1,13	3,53	1,07	3,58	1,31	3,92	1,08
	relação custo/ benefício	3,37	1,13	3,35	1,27	3,42	1,00	3,33	1,15
	falta de conhecimento	**3,71**	**1,15**	**3,65**	**1,11**	**3,92**	**1,31**	3,58	1,08
	cultura organizacional	3,66	1,02	3,41	1,12	3,67	0,98	**4,00**	**0,85**

Na análise referente à quantidade de computadores que as empresas pesquisadas possuem, novamente o fator “evitar perdas financeiras” se confirmou com a maior média matemática e também após realização dos testes estatísticos, conforme as tabelas 15 e 16.

Tabela 15: teste *Kruskal Wallis – Quantidades de Computadores*

quantidade	*valor de p fatores motivadores*	*valor de p fatores inibidores*
até 10	0,158	0,842
de 11 a 20	0,199	0,600
acima de 20	0,003	0,415

Tabela 16: teste *Mann-Whitney – Acima de 20 micros*

Fatores	*Mann-Whitner U*	*Wilcoxon W*	*Z*	*Asymp.Sig (2-tailed)*
especialista interno x incidente anterior	71,400	149,500	-0,030	0,976
especialista interno x consciência do gestor	41,500	119,500	-1,898	0,058
especialista interno x evitar perdas financeiras	17,000	95,000	-3,481	0,000
incidente anterior x evitar perdas financeiras	27,000	105,000	-2,855	0,004
consciência do gestor x evitar perdas financeiras	38,000	116,000	-2,215	0,027

Os fatores inibidores novamente não apresentaram diferenças significativas entre suas médias, porém é válido observar no gráfico 23 que o fator inibidor se altera dependendo da quantidade de computadores que a empresa possui, sendo

para as empresas com até 10 micros e de 11 a 20 micros a “falta de conhecimento” e para as que possuem acima de 20 micros a “cultura organizacional”.

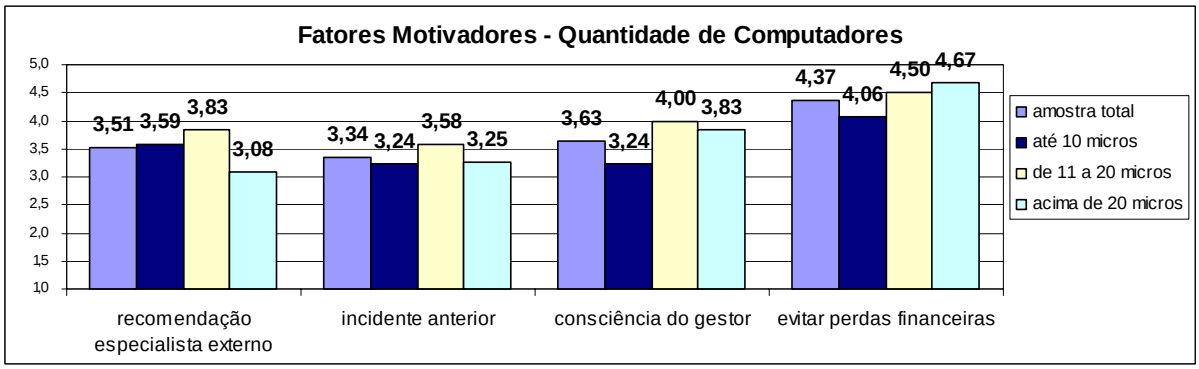

Gráfico 22: fatores motivadores na análise quantidade de computadores

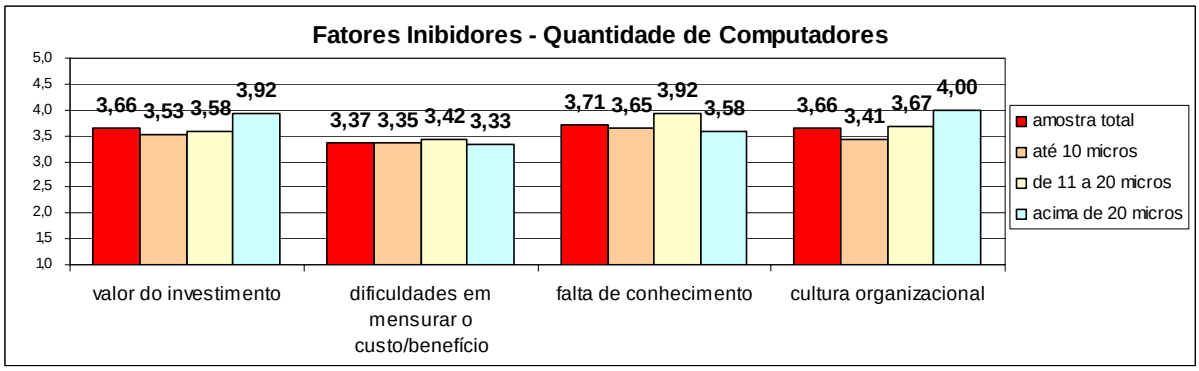

Gráfico 23: fatores inibidores na análise quantidade de computadores

4.5.4 NÍVEL DE INFORMATIZAÇÃO DOS NEGÓCIOS

Tabela 17: nível de informatização dos negócios

Fatores		Amostra		Baixo		Médio		Alto	
		média	σ	média	σ	média	σ	média	σ
motivadores	especialista externo	3,51	1,12	3,25	1,26	3,52	1,05	3,64	1,29
	incidente anterior	3,34	1,24	3,00	0,82	3,30	1,35	3,36	1,29
	consciência do gestor	3,63	1,13	3,25	1,26	3,67	1,24	3,82	0,87
	evitar perdas financeiras	**4,37**	**0,83**	**4,00**	**0,82**	**4,41**	**0,89**	**4,45**	**0,69**
inibidores	valor do investimento	3,66	1,13	3,25	0,50	3,74	1,16	**3,64**	**1,21**
	relação custo/ benefício	3,37	1,13	3,25	0,50	3,48	1,25	3,18	0,98
	falta de conhecimento	**3,71**	**1,15**	**4,00**	**0,82**	3,74	1,10	3,64	1,43
	cultura organizacional	3,66	1,02	3,25	0,50	**3,81**	**1,08**	3,45	0,93

A última análise feita foi em relação ao nível de informatização dos negócios. O fator motivador “evitar perdas financeiras” prevaleceu sobre todos os demais e os fatores inibidores novamente não apresentaram diferença significativa. A tabela 18 exiba os resultados do teste *Kruskal Wallis* para verificar as diferenças entre as médias, somente na amostra de empresas com nível de informatização médio houve diferenças significativas entre as médias, nas outras análises – nível de informatização baixo e alto – tanto os fatores motivadores como inibidores tem o mesmo peso na adoção da gestão da segurança da informação. A tabela 19 confirma o fator motivador “evitar perdas financeiras”.

Tabela 18: teste *Kruskal Wallis – Nível de Informatização dos Negócios*

nível de informatização	*valor de p fatores motivadores*	*valor de p fatores inibidores*
baixo	0,489	0,298
médio	0,004	0,774
alto	0,130	0,600

Tabela 19: teste *Mann-Whitney – Nível de Informatização Médio*

Fatores	*Mann-Whitner U*	*Wilcoxon W*	*Z*	*Asymp.Sig (2-tailed)*
especialista interno x incidente anterior	328,500	706,500	-0,643	0,521
especialista interno x consciência do gestor	327,000	705,000	-0,672	0,501
especialista interno x evitar perdas financeiras	195,500	573,500	-3,115	0,002
incidente anterior x evitar perdas financeiras	192,500	570,500	-3,193	0,001
consciência do gestor x evitar perdas financeiras	238,000	616,000	-2,373	0,018

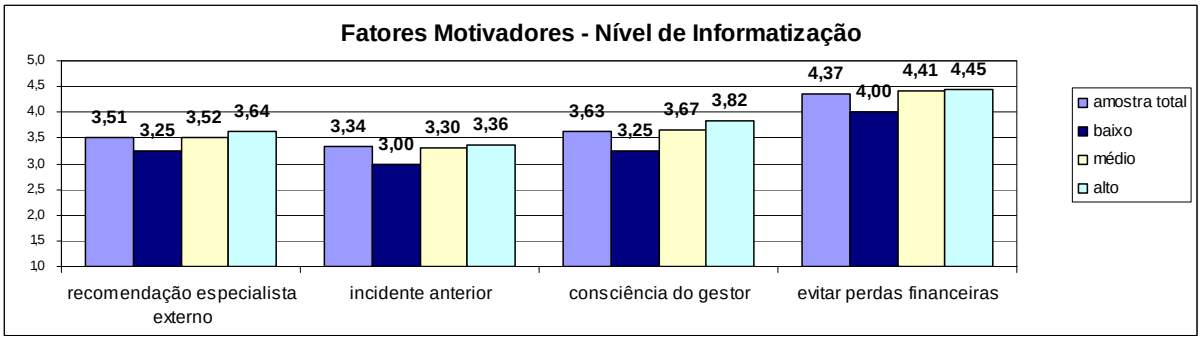

Gráfico 24: fatores motivadores na análise nível de informatização

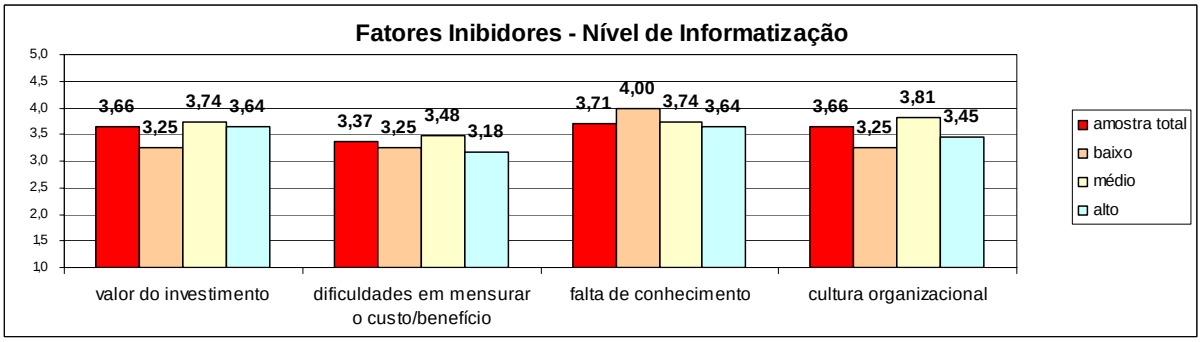

Gráfico 25: fatores inibidores na análise nível de informatização

5 CONCLUSÃO

Este trabalho respondeu à seguinte pergunta: Que fatores são capazes de influenciar a adoção da gestão da segurança da informação por pequenas e médias empresas?

Para tanto, foram entrevistados sete gestores a fim de entender suas preocupações com a gestão da segurança da informação e para fornecer subsídios para criação do questionário. O questionário on-line foi respondido por 43 empresas do ramo de fabricação de produtos de metal e apresentou os seguintes resultados:

- evitar perdas financeiras foi o fator motivador para adoção de gestão da segurança da informação que apresentou maior média e o único que apresentou diferença significativa das médias comparando com os demais fatores. O fator reforça a preocupação constante das empresas em evitar perdas principalmente financeiras ou reduzir custos. Os demais fatores motivadores, conforme comprovaram os testes estatísticos, podem ser considerados com pesos iguais.

- não foi possível indicar o principal fator inibidor na adoção da gestão da segurança da informação, pois os testes estatísticos revelaram que todos os fatores possuíam o mesmo nível de significância. Porém, nas entrevistas realizadas com os gestores a falta de conhecimento apareceu como um possível fator inibidor e após a realização das pesquisas quantitativas apresentou a maior média matemática.

Outro objetivo era avaliar através dos controles descritos na norma brasileira de segurança - ABNT NBR ISO/IEC 17799:2005 - se a empresa possuía gestão da segurança da informação.

Das empresas pesquisadas, 80% possuem pelo menos um controle em cada uma das camadas de segurança: física, lógica e humana. Essa porcentagem diminui para 59% quando avaliado se possuem pelo menos metade dos controles pesquisados implantados. A ferramenta mais utilizada foi o antivírus, presente em todas das empresas pesquisadas.

A camada humana foi a que apresentou o menor índice de ferramentas/técnicas implantadas pelas empresas pelo número de controles

pesquisados nesta camada. As empresas ainda se preocupam mais com controles tecnológicos para diminuir o risco de incidentes de segurança da informação.

A pesquisa também verificou a porcentagem dos controles, independente da camada, as empresas pesquisadas possuíam. Das 41 empresas pesquisadas, 21 possuem menos ou 60% dos controles pesquisados presentes na ISO/IEC 17799:2005.

Em relação às seções da norma ISO/IEC 17799:2005 foi verificada uma baixa adequação das pequenas e médias empresas, o que pode demonstrar que a norma requer muitos controles que a maioria não está preocupada em implantar ou não possuem tempo ou dinheiro para isso. Contando que a norma sugere 127 controles e neste trabalho foram selecionados somente 20, esperava-se uma grande adequação aos controles.

O presente estudo mostrou que as pequenas e médias empresas, apesar de considerarem a perda financeira como o principal fator para adoção da gestão da segurança da informação, são carentes de informações sobre a correta gestão da segurança da informação.

Para estudos futuros, recomenda-se aplicar a pesquisa em outros setores da economia como empresas de: serviços ou comércio, a fim de verificar a amplitude das análises. Uma amostra maior de empresas também poderia relevar maiores informações e possibilitar indicar um fator inibidor.

Recomendam-se também estudos para verificar a causa da falta de conhecimento dos gestores em gestão da segurança da informação e TI, haveria uma falta de interesse por parte das empresas ou dos gestores?

6 REFERÊNCIAS

ADACHI, Tomi. **Gestão de Segurança em Internet Banking** – São Paulo: FGV, 2004. 121p. Mestrado. Fundação Getúlio Vargas – Administração. Orientador: Eduardo Henrique Diniz.

_____; DINIZ, Eduardo Henrique. **Gestão de Segurança em Internet Banking: um estudo de casos múltiplos no Brasil**. ENANPAD - 29º Encontro da ANPAD, 2005.

ALBERTIN, Alberto Luiz. **Administração de Informática: funções e fatores críticos de sucesso** – São Paulo: Atlas, 2004.

APPOLINÁRIO, Fabio. **Metodologia da Ciência: filosofia e prática da pesquisa** – São Paulo: Pioneira Thomson Learning, 2006.

BANTEL, Guilherme. **Fraudes virtuais crescem 1.313% no Brasil** – IDG Now: 08/07/2005 – 12h14. Disponível em: <http://www.idgnow.uol.com.br>.

BEAL, Adriana. **Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações** – São Paulo: Atlas, 2005.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em Informática e de Informações** – São Paulo: Editora SENAC São Paulo, 1999.

CERNEV, Adrian Kemmer; LEITE, Jaci Corrêa. **Segurança na Internet: a percepção dos usuários como fator de restrição ao comércio eletrônico no Brasil** – ENANPAD, 2005.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Pesquisa sobre o uso das tecnologias da informação e da comunicação no Brasil 2005**. Disponível em <http://www.mct.gov.br/upd_blob/10819.pdf>. Acesso em 27/12/2006 às 20h48min.

COMPUTERWORLD. **SMBs brasileiras investem US$ 260 mi em segurança em 2007** – ComputerWorld, 21/11/2006 às 08h05. Disponível em <http://computerworld.uol.com.br/ seguranca/2006/11/21/idgnoticia.2006-11-20.6002581207/IDGNoticia_view>. Acesso em 28/12/2006 às 12h10.

CRAGG, Paul B.; KING, Malcolm. **Small-Firm Computing: motivators and inhibitors** – MIS Quarterly, março/1993, pg. 47-60.

FONTES, Edison. **Segurança da Informação: o usuário faz a diferença** - São Paulo: Saraiva, 2006.

GABBAY, Max Simon. **Fatores influenciadores da implementação de ações de Gestão de Segurança da Informação: um estudo com executivos e gerentes de tecnologia da informação em empresas do Rio Grande do Norte**. 01/06/2003. 1v. 150p. Mestrado. Universidade Federal do Rio Grande do Norte - Engenharia de Produção. Orientador(es): Anatália Saraiva Martins Ramos. Biblioteca Depositaria: BCZM

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa** – São Paulo: Atlas, 2002.

GUPTA, Atul; HAMMOND, Rex. **Information systems security issues and decisions for small business: an empirical examination** – Information Management & Computer Security, 2004, pg. 297-310. Disponível em <http://www.emeralinsight.com/0968-5227.htm>. Acesso em 09/09/2006.

HAIR, JR Joseph F.; BABIN, Barry; MONEY Arthur H.; SAMOUEL, Phillip. **Fundamentos de Métodos de Pesquisa em Administração** - Porto Alegre: Bookman, 2005.

HITT, Michael A.; IRELAND, R. Duane; HOSKISSON, Robert E. **Administração Estratégica** – São Paulo: Pioneira Thomson Learning, 2005.

HOLANDA, Roosevelt de. **O estado da arte em sistemas de gestão da segurança da Informação: Norma ISO/IEC 27001:2005** – São Paulo: Módulo Security Magazine, 19 jan 2006. Disponível em <http://www.modulo.com.br>.

ISO 17799. **ABNT NBR ISO/IEC 17799:2005** – Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Associação Brasileira de Normas Técnicas – Rio de Janeiro: ABNT, 2005.

MESQUITA, Renata. **Ataques hackers triplicaram no 1º trimestre** - Plantão INFO: 30/04/2003 – 09h49. Disponível em <http://www.infoexame.com.br>.

MITNICK, Kevin D.; SIMONS, William L. **A Arte de Enganar: ataques de hackers: controlando o fator humano na segurança da informação** – São Paulo: Pearson Education, 2003.

MÓDULO. **9ª Pesquisa Nacional de Segurança da Informação** – Rio de Janeiro: Outubro/2003. Disponível em <http://www.modulo.com.br>.

MORAES, Giseli Diniz de Almeida; TERENCE, Ana Claúdia Fernandes; ESCRIVÃO FILHO, Edmundo. **A tecnologia da informação como suporte à gestão estratégica da informação na pequena empresa** – Revista de Gestão da Tecnologia e Sistemas da Informação, v.1, n.1, 2004, pg. 28-44.

NERY, Fernando; PARANHOS, Maurício. *COBIT ou ISO 17799? Iniciando a reflexão* - Módulo Security Magazine, 23/09/2003. Disponível em http://www.modulo.com.br.

LUNARDI, Guilherme Lerch; DOLCI, Pietro Cunha. **Adoção de Tecnologia da Informação e seu Impacto no Desempenho Organizacional: um estudo realizado com micro e pequenas empresas** – Salvador: ENANPAD - 30º Encontro da ANPAD, 2006.

OLIVA, Rodrigo Polydoro; OLIVEIRA, Mírian. **Elaboração, Implantação e Manutenção de Política de Segurança por Empresas no Rio Grande do Sul em relação às recomendações da NBR/ISO17799** – ENANPAD, 2003.

PALVIA, Prashant C.; PALVIA, Shailendra C. **An examination of the IT satisfaction of small-business users.** Information & Management. Amsterdam: Mar 8, 1999.Vol.35, Iss. 3; pg. 127, 11 pgs

PRATES, Gláucia Aparecida; OSPINA, Marco Túlio. **Tecnologia da Informação em Pequenas Empresas: fatores de êxito, restrições e benefícios** – RAC, v.8, n.2, Abr/Jun-2004, pg. 09-26.

ROCHA, Luís Fernando. **Governança em TI e Segurança: COBIT e ISO 17799 no mercado financeiro** – Modulo Security Magazine, 29/09/2003. Disponível em <http://www.modulo.com.br>.

SANTOS JR., Silvio; FREITAS, Henrique; LUCIANO, Edimara Mezzomo. **Dificuldades para o uso da tecnologia da informação** – RAE Eletrônica, v.4, n.2, art.20, jul/dez-2005.

SCHNEIER, Bruce. **Segurança.com: segredos e mentiras sobre a proteção na vida digital** – Rio de Janeiro: Campus, 2001.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva** – Rio de Janeiro: Campus, 2003.

VALIM, Carlos Eduardo. **Polícia Civil cobra informações sobre fraudes** – ComputerWorld: 27/04/2005 – 16h26. Disponível em <http://www.computerworld.uol.com.br>.

APÊNDICE

QUESTIONÁRIO

Grupo de variáveis e seu construto

Grupo de Variáveis	Enunciado	Opções de Resposta	Fonte
Perfil do Gestor	Por favor, informe seu e-mail:	aberta	
Perfil do Gestor	Escolha abaixo o cargo que mais se aproxima do seu:	cargo: sócio-proprietário, diretor, gerente, supervisor, analista	
Perfil do Gestor	Qual é seu departamento?	departamento: presidência/ gerência geral, finanças, tecnologia da informação, suprimentos, engenharia, contabilidade, comercial (vendas), qualidade, rh, jurídico, auditoria	
Perfil do Gestor	Selecione abaixo a opção que melhor descreve o seu envolvimento nos processos de aquisição de produtos ou serviços em Tecnologia da Informação e/ou Gestão da Segurança da Informação:	a decisão é minha; a decisão final não é minha, mas contribuo, não participo do processo	
Perfil da Empresa	Qual o número total de funcionários de sua empresa?	01 a 09, 10 a 49, 50 a 99, 100 a 499, acima de 500	
Perfil da Empresa	Qual a quantidade de computadores em uso?	menos de 5, de 5 a 10, de 10 a 20, de 21 a 100, de 101 a 500, acima de 500	Santos Jr, Freitas e Luciano (2005)
Perfil da Empresa	Na sua empresa a responsabilidade pela área de Tecnologia da Informação (TI) é de:	um departamento interno, uma empresa terceira com contrato, uma empresa terceira com chamadas eventuais	
Perfil da Empresa	Quanto ao nível de informatização da sua empresa você o considera:	baixo (edição de documentos, e-mails, acesso a internet); médio (nível baixo + uso intensivo de planilha eletrônicas, Internet *Banking*); alto (nível médio + sistema integrado, acesso remoto a funcionários/ fornecedores, comércio eletrônico)	Gabbay (2003)

Ferramentas e Técnicas	Atribua uma nota relativa ao grau de importância atribuído pela sua empresa às ferramentas ou técnicas de Segurança da Informação. Quanto maior a nota mais importante para sua empresa. Classificação da informação no formato físico e no formato eletrônico (ex: confidencial, restrita, interna, pública)	nota de 1 a 5, se a empresa possui ou não	Beal (2005), Caruso e Steffen (1999), Módulo (2003), ISO 17799 (2005)
Ferramentas e Técnicas	Regras para uso da informação e dos recursos de TI (internet, e-mail, ...)	nota de 1 a 5, se a empresa possui ou não	ISO 17799 (2005)
Ferramentas e Técnicas	Sala de servidores protegida e em local restrito	nota de 1 a 5, se a empresa possui ou não	Caruso e Steffen (1999), ISO 17799 (2005)
Ferramentas e Técnicas	Equipamento para proteção de falhas na energia elétrica (ex: *no-break*)	nota de 1 a 5, se a empresa possui ou não	Módulo (2003), ISO 17799 (2005)
Ferramentas e Técnicas	Antivírus	nota de 1 a 5, se a empresa possui ou não	Caruso e Steffen (1999), Módulo (2003), ISO 17799 (2005)
Ferramentas e Técnicas	Sistema de backup (cópia de segurança)	nota de 1 a 5, se a empresa possui ou não	Beal (2005), Caruso e Steffen (1999), Módulo (2003), ISO 17799 (2005)
Ferramentas e Técnicas	Firewall (proteção da rede local contra acessos indevidos)	nota de 1 a 5, se a empresa possui ou não	ISO 17799 (2005)
Ferramentas e Técnicas	Descarte seguro da mídia removível (ex: disquete, CD, DVD, ...) e documentação de sistemas quando não forem mais necessárias, usando incineração ou trituração	nota de 1 a 5, se a empresa possui ou não	ISO 17799 (2005), Sêmola (2003)
Ferramentas e Técnicas	Monitoramento e análise crítica dos registros (logs) de auditoria com atividades dos usuários, exceções e outros eventos de segurança da informação	nota de 1 a 5, se a empresa possui ou não	ISO 17799 (2005)
Ferramentas e Técnicas	Canais de comunicação para registro e notificação de fragilidades e eventos de segurança da informação (ex: intranet, formulários, telefone de suporte)	nota de 1 a 5, se a empresa possui ou não	ISO 17799 (2005)
Ferramentas e Técnicas	Nome de usuário, senha individual e secreta para acesso a rede	nota de 1 a 5, se a empresa possui ou não	Caruso e Steffen (1999), ISO 17799 (2005)
Ferramentas e Técnicas	Uso de criptografia em banco de dados e/ou para troca de informações (ex: (certificados de chaves públicas, assinaturas digitais)	nota de 1 a 5, se a empresa possui ou não	Adachi (2005), ISO 17799 (2005)
Ferramentas e Técnicas	Supervisão do desenvolvimento terceirizado de software com requisitos para controles de segurança da informação	nota de 1 a 5, se a empresa possui ou não	Beal (2005), ISO 17799 (2005)
Ferramentas e Técnicas	Atualização de software para correção de falhas de segurança e/ou vulnerabilidades técnicas (ex: Windows Update)	nota de 1 a 5, se a empresa possui ou não	ISO 17799 (2005)

Ferramentas e Técnicas	Política de segurança da informação formalizada com apoio da direção e divulgação a todos os funcionários	nota de 1 a 5, se a empresa possui ou não	Beal (2005), ISO 17799 (2005), Sêmola (2003), Caruso e Steffen (1999)
Ferramentas e Técnicas	Contratos e acordos com terceiros contendo termos claros relativos a segurança	nota de 1 a 5, se a empresa possui ou não	ISO 17799 (2005)
Ferramentas e Técnicas	Conscientização, educação e treinamento em segurança da informação (ex: palestras, cursos, cartazes, ...)	nota de 1 a 5, se a empresa possui ou não	Fontes (2006), ISO 17799 (2005)
Ferramentas e Técnicas	Plano formalizado de recuperação de desastres e contingência, visando a continuidade do negócio da organização	nota de 1 a 5, se a empresa possui ou não	ISO 17799 (2005)
Ferramentas e Técnicas	Controle dos direitos de propriedade intelectual (software, documentos, projetos, marcas, patentes, licenças de código-fonte) de acordo com requisitos legais	nota de 1 a 5, se a empresa possui ou não	ISO 17799 (2005)
Ferramentas e Técnicas	Aviso aos usuários sobre o monitoramento dos recursos de TI, de forma a dissuadi-los a usá-los para propósitos não autorizados e garantir que a organização está em conformidade com a lei	nota de 1 a 5, se a empresa possui ou não	Fontes (2006), ISO 17799 (2005)
Fator Motivador	Recomendação de um especialista externo ou fornecedor da área	nota de 1 a 5	Entrevista, Thong (2004), Cragg e King (1993)
Fator Motivador	Incidente de segurança ocorrido anteriormente	nota de 1 a 5	Entrevista, Gabbay (2003), Gupta e Hammond (2004)
Fator Motivador	Consciência do próprio gestor	nota de 1 a 5	Palvia e Palvia (1999)
Fator Motivador	Para evitar possíveis perdas financeiras ou operacionais	nota de 1 a 5	Entrevista
Fator Inibidor	Valor do investimento	nota de 1 a 5	Prates e Ospina (2004)
Fator Inibidor	Dificuldade em mensurar a relação custo/benefício do investimento	nota de 1 a 5	Entrevista, Módulo (2003)
Fator Inibidor	Falta de conhecimentos sobre ferramentas ou técnicas de defesa	nota de 1 a 5	Entrevista, Prates e Ospina (2004)
Fator Inibidor	Cultura organizacional	nota de 1 a 5	Lunardi e Dolci (2006)